it management

Der Motor für Innovation
Juli/August 2024

INKLUSIVE 48 SEITEN
it security

CS Campana Schott

KI-Transformation
ab Seite 24

AKTE XZ-BACKDOOR

Cybersicherheit in der Software Supply Chain

Alexander Bluhm, genua GmbH

CLOUD COST MANAGEMENT

Unverzichtbare FinOps

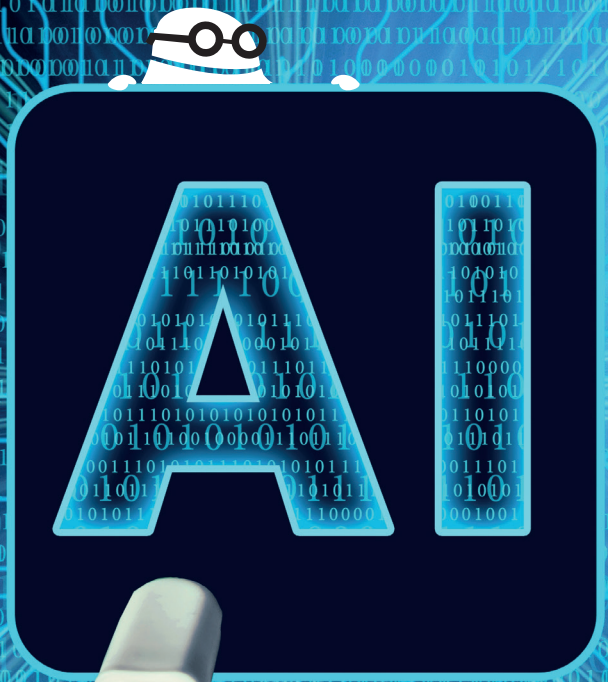
NACHHALTIGE PRODUKTION

Hand in Hand in die Zukunft

CONSOLIDATION & FINANCIAL ANALYTICS

Bindeglied zum ERP

Fluch oder Segen?



SCAN ME

it-daily.net/ki

Mehr Infos dazu im Printmagazin

itmanagement

und online auf www.it-daily.net

BLINDE FLECKEN

LIEBE LESERINNEN UND LESER,

die verheißungsvollen Versprechungen moderner Technologien überstrahlen gerne die schattigen Kehrseiten und bringen zahlreiche blinde Flecke mit sich. Fälle wie die XZ-Backdoor zogen auch die Risiken undurchsichtiger Software-Lieferketten ins Rampenlicht. Überhaupt durchdringt ein komplexes Geflecht aus Code-Modulen unzähliger Drittanbieter unsere IT-Systeme – ein gefundenes Fressen für Cyberkriminelle.

Doch die Probleme beschränken sich nicht nur auf die Sicherheit. Studien zufolge verpuffen 30 Prozent der Cloud-Budgets durch ungenutzte Kapazitäten. Budgetdisziplin ist hier ein Fremdwort, Transparenz oft ein frommer Wunsch. Was einst als grenzenlose Skalierbarkeit gepriesen wurde, entpuppt sich für viele als Kostenfalle, die zu hohen Ausgaben führen kann.

IT-Manager müssen jetzt die Führung übernehmen, um Klarheit in den verworrenen IT-Labyrinthen zu schaffen. Transparenz und Kontrolle sind dabei nicht nur wünschenswert, sondern notwendig.

KI und Automatisierung etwa bieten uns die Werkzeuge, um diese Herausforderungen zu meistern. Sie ermöglichen es, kritische Schwachstellen und Kostentreiber zu identifizieren und zu eliminieren. Doch der wahre Schlüssel zum Erfolg liegt in einem ganzheitlichen Umdenken: Nur durch Wachsamkeit und Aufklärung können Organisationen den blinden Flecken wirksam begegnen. Bleiben Sie also informiert!

Herzlichst,

Lars Becker | Redakteur

INHALT

COVERSTORY

FINANCE SPEZIAL

IT MANAGEMENT

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

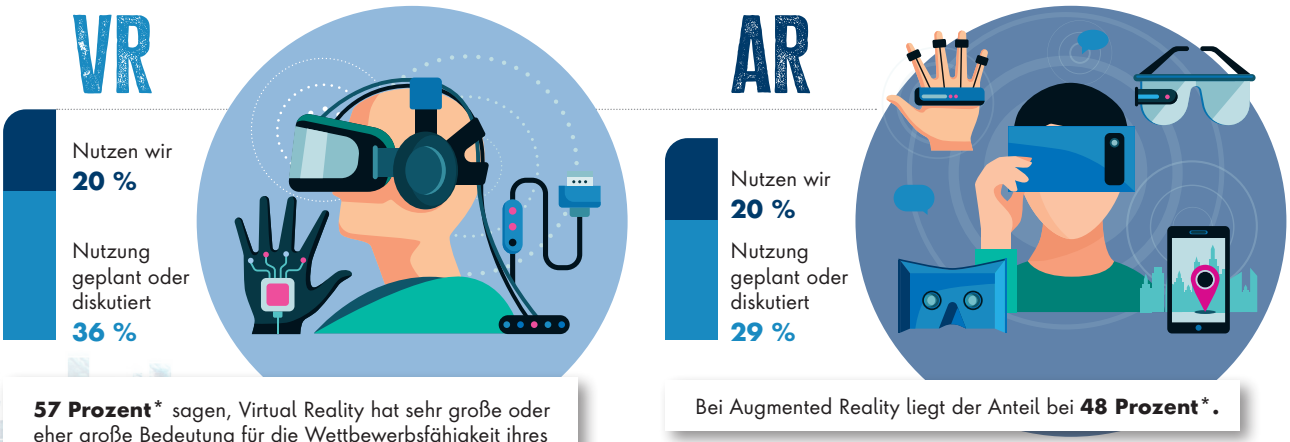
Inklusive 48 Seiten it security

GUT ZU WISSEN

Achten Sie auf dieses Icon und lesen sie mehr zum Thema im Internet auf **www.it-daily.net**

VIRTUAL UND AUGMENTED REALITY SIND BEREITS WEIT VERBREITET

Welche der Technologien nutzen Sie in Ihrem Unternehmen oder planen/diskutieren Sie zu nutzen?



57 Prozent* sagen, Virtual Reality hat sehr große oder eher große Bedeutung für die Wettbewerbsfähigkeit ihres Unternehmens.

Bei Augmented Reality liegt der Anteil bei **48 Prozent***.

*Bedeutung insgesamt
Basis: Alle Unternehmen (n=605) | Quelle: Bitkom Research 2024

AUGMENTED ODER VIRTUAL REALITY?

UNTERNEHMEN SETZT BEREITS AR- ODER VR-TECHNOLOGIE EIN

Bei der Wartung einer Turbine die Schritt-für-Schritt-Anleitung direkt vor Augen haben oder die neue Werkhalle schon lange vor Fertigstellung im virtuellen Probebetrieb betrachten – das ist mit Augmented und Virtual Reality heute bereits möglich. Jedes fünfte Unternehmen (20 Prozent) nutzt bereits einzelne VR- oder AR-Anwendungen. Weitere 36 Prozent planen oder diskutieren den Einsatz von VR im Unternehmen, bei AR sind es 29 Prozent. Das sind Ergebnisse einer repräsentativen Befragung von 605 Unternehmen ab 20 Beschäftigten in Deutschland im Auftrag des Digitalverbands Bitkom.

„Die lange Zeit von Science-Fiction-Filmen geprägte Vorstellung von Augmented und Virtual Reality ist in einigen Bereichen der Wirtschaft bereits Realität", sagt Niklas Veltkamp, Mitglied der Bitkom-Geschäftsleitung.

Bei Augmented Reality stehen Schulung, Ausbildung und Weiterbildung ganz oben auf der Liste der Anwendungen, zwei Drittel (64 Prozent) der Unternehmen, die AR einsetzen oder dies derzeit planen oder diskutieren, nennen diesen Bereich. Knapp dahinter folgen Konstruktion und Planung (60 Prozent). Mit deutlichem Abstand liegt Kollaboration (36 Prozent) auf Platz drei, vor dem Einsatz im Marketing und für Messen (34 Prozent). Jeweils rund ein Fünftel nennt Fernwartung (22 Prozent) sowie Schritt-für-Schritt-Anleitungen (19 Prozent). Der Verkauf kommt auf 16 Prozent, die Einarbeitung neuer Mitarbeiter auf 10 Prozent und nur 1 Prozent geben Navigation oder Orientierungshilfe an.

Bei Virtual Reality liegt das Haupteinsatzgebiet aus Sicht der Unternehmen, die die Technologie einsetzen, dies planen oder diskutieren im Bereich der Konstruktion und Planung (74 Prozent). Dahinter folgen Schulung, Ausbildung und Weiterbildung (61 Prozent), Kollaboration (46 Prozent), Marketing und Messen (37 Prozent) sowie der Verkauf (14 Prozent). Schlusslicht beim VR-Einsatz ist die Einarbeitung neuer Mitarbeiterinnen und Mitarbeiter (5 Prozent).

www.bitkom.org

Organizational Change Management

4 SCHRITTE, UM KÜNSTLICHE INTELLIGENZ EFFEKTIV ZU VERWALTEN

Künstliche Intelligenz (KI)-Systeme werden in einer Vielzahl von Anwendungen eingesetzt, darunter Automatisierung, Entscheidungsunterstützung und Datenanalyse. Um KI jedoch erfolgreich einzusetzen, ist ein effektives Organizational Change Management (OCM) erforderlich. OCM ist ein Prozess zur Überwachung, Verwaltung und Optimierung von IT-Systemen und -Prozessen. Es gewährleistet sowohl die Verfügbarkeit als auch die Sicherheit des KI-Systems. Daneben optimiert es die Leistung der KI.

OCM für KI ist für Unternehmen aller Größen und Branchen wichtig, die KI-Systeme einsetzen oder planen, diese einzusetzen. Insbesondere Unternehmen, die KI in kritischen Anwendungen einsetzen, wie in der Finanzindustrie oder im Gesundheitswesen, sollten ein OCM für KI implementieren. Es gewährleistet die Verfügbarkeit ihrer KI-Systeme, damit diese 24/7 einsatzbereit sind ebenso wie die Sicherheit ihrer KI-Systeme, damit diese vor Angriffen geschützt sind. Dies ist wichtig, da KI-Systeme oft Zugang zu sensiblen Daten haben. Zudem hilft OCM die Leistung der KI-Systeme zu optimieren, damit diese effizient und effektiv arbeiten. Es automatisiert Aufgaben und stellt Echtzeit-Monitoring bereit.

4 Schritte eines OCM für eine effektive KI-Systemverwaltung

1 **Anforderungen definieren:** Unternehmen sollten zunächst ihre Anforderungen an ein OCM für KI definieren. Dies umfasst die Art und Weise, wie KI-Systeme im Unternehmen eingesetzt werden, sowie die gewünschten Ziele für das OCM.

2 **Tools und Technologien auswählen:** Unternehmen sollten dann die richtigen Tools und Technologien für ihre Anforderungen auswählen. Es gibt eine Vielzahl von OCM-Lösungen auf dem Markt, die auf verschiedene Bedürfnisse zugeschnitten sind.

3 **Team zusammenstellen:** Unternehmen sollten ein Team von KI-Experten zusammenstellen, die das OCM betreiben und verwalten.

4 **Implementieren und testen:** Unternehmen sollten ihr OCM implementieren und kontinuierlich testen, um sicherzustellen, dass es die gewünschten Ziele erreicht.

www.unisys.com

Cookie Alternative

DATEN SIND DIE LIEBLINGSWÄHRUNG IM INTERNET

Zwei von drei Bundesbürgern verzichten konsequent darauf, kostenpflichtige Webseiten oder Apps zu nutzen. 86 Prozent sind dafür bereit, im Internet mit ihren Daten zu zahlen. Obwohl sie zugeben, kaum zu wissen, welche Informationen dabei über sie gespeichert werden. Das zeigt eine aktuelle bevölkerungsrepräsentative Befragung von The Trade Desk unter 1.500 Bundesbürgern.

95 Prozent der Befragten haben nach eigener Aussage kein klares Bild davon, welche Informationen über sie gesammelt werden. Dennoch sind sie nicht naiv. Ihnen ist bekannt, dass sie online unzählige Datenspuren hinterlassen – insbesondere auf Shopping-Webseiten und in den sozialen Netzwerken.

Cookies gelten als aufdringlich und intransparent

Da die Wertschöpfung über das Internet weiter stark wächst, müssen neue Alternativen zur Identifizierung vor allem auch den Wünschen der Nutzer Rechnung tragen. Sowohl Verbraucherschützer als auch die Mehrheit der befragten Bundesbürger fordern vor allem Transparenz. 78 Prozent finden Cookies aufdringlich und begrüßen eine andere Form der Datenweitergabe.

Nach Überzeugung von The Trade Desk sollte es künftig eine Open-Source-„Datenwährung" für das Internet geben, die den Nutzern mehr Transparenz und Kontrolle über ihre Daten gibt, den Medienhäusern angemessene Einnahmen für ihre Inhalte ermöglicht und auf die Europäische Union zugeschnitten ist: die European Unified ID oder EUID. Diese Identitätslösung basiert auf einer E-Mail-Adresse, die verschlüsselt und pseudonymisiert ist.

Die Studienergebnisse zeigen: Ist dies gewährleistet, sind 60 Prozent der Befragten bereit, ihre E-Mail-Adresse anstelle von Cookies zu verwenden. Der Nutzer kann über diese Methode direkt einsehen und steuern, welchen Medien er eine Datennutzung gestatten möchte. Durch die Wiedererkennung der entsprechenden ID kann auf allen Kanälen zielgruppengerechte Werbung ausgespielt werden. Das System ist bereits im Einsatz und viele große Werbetreibende, Medienhäuser sowie Handelsunternehmen arbeiten mit einer solchen, auf die Europäische Union zugeschnittenen Identity-Lösung.

www.thetradedesk.com/de

(Quelle: The Trade Desk Intelligence, Mai 2024)

HYBRIDTECHNOLOGIE

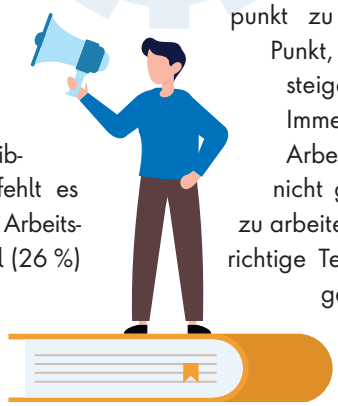
MITARBEITERZUFRIEDENHEIT IM FOKUS

Eine aktuelle Studie zeigt, dass die Mehrheit der Unternehmen nicht über die notwendigen Technologien verfügt, um flexibles Arbeiten zu unterstützen. Nur 29 Prozent der deutschen Arbeitnehmer geben an, dass sie über alle Technologien verfügen, um nahtlos mit anderen Kollegen zusammenarbeiten zu können.

Für die Studie, die von Opinion Matters im Auftrag von Ricoh Europe durchgeführt wurde, wurden 1.000 Arbeitnehmer und 300 Führungskräfte in Deutschland befragt. Die Ergebnisse zeigen, dass flexibles Arbeiten für deutsche Arbeitnehmer nach wie vor höchste Priorität hat.

So nannten die Arbeitnehmer flexiblere Arbeitsregelungen bei einem neuen Arbeitgeber als Hauptgrund dafür, dass sie in den nächsten zwölf Monaten eine Kündigung in Erwägung ziehen. Dazu gehört die Möglichkeit, den Arbeitstag im Vorfeld planen zu können und sicherzustellen, dass die Anforderungen bezüglich Arbeitsplatzinfrastruktur, Standort und Arbeitsplatztechnologie erfüllt werden.

Trotz der Bedeutung, die die Beschäftigten dem flexiblen Arbeiten beimessen, fehlt es vielen an grundlegenden Arbeitsmitteln. Mehr als ein Viertel (26 %) der Beschäftigten hat keinen Zugang zu Collaboration-Software wie Microsoft Teams und Zoom, während 32 Prozent keinen Zugang zu Collaboration-Hardware/Hybrid-Meeting-Technologien (AV-Technologien wie Videokonferenzen) haben, obwohl diese nachgefragt werden.



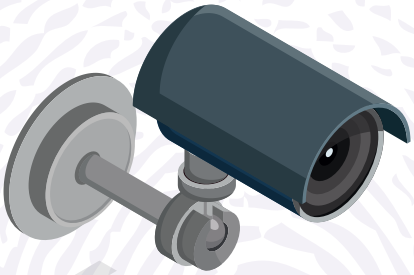
Die Führungskräfte sind sich des Problems bewusst: 27 Prozent räumen ein, dass ihre Tools für die Zusammenarbeit nicht den Erwartungen entsprechen, was es den Mitarbeitern erschwert, ihre tägliche Arbeit zu erledigen. Trotzdem nennt nur einer von fünf Entscheidungsträgern (20 %) die Verbesserung der Mitarbeitererfahrung als strategische Priorität für das kommende Jahr.

Die Studie veranschaulicht zugleich, an welchen Stellschrauben Führungskräfte in diesem Jahr drehen sollten, um die Zufriedenheit ihrer Mitarbeiter in den Mittelpunkt zu rücken. Der wichtigste Punkt, um die Zufriedenheit zu steigern, ist flexibles Arbeiten. Immerhin ein Viertel (25 %) der Arbeitnehmer gibt an, dass sie nicht gezwungen sind, im Büro zu arbeiten, sondern dass ihnen die richtige Technologie zur Verfügung gestellt wird, damit sie dort arbeiten können, wo es für sie am besten ist.

www.ricoh.de

Security by Design

SICHERE IT-SYSTEME REALISIEREN



Die Zahl der Angriffe auf Systeme, Anwendungen und Infrastrukturen steigt unaufhörlich, und die Schadenssummen für die Anwenderunternehmen steigen mit. Allein in Deutschland entstanden laut Bitkom im Jahr 2023 Schäden in Höhe von über 200 Milliarden Euro - eine Verdoppelung gegenüber 2019. Und das, obwohl auch die IT- und insbesondere die Security-Budgets in Unternehmen und Behörden kontinuierlich erhöht werden. Offensichtlich hat man in den Unternehmen die Gefahr erkannt, die Mittel bereitgestellt - aber das Problem trotzdem nicht in den Griff bekommen. Zeit für eine Analyse.

IT-Systeme sind komplex. Neue Infrastrukturen müssen viele Vorgaben erfüllen - aktuelle und meist auch zukünftige. IT-Security steht oft nicht an erster Stelle dieser Anforderungen. Sie soll häufig erst später nachgerüstet werden, um die Systeme gegen Angriffe immun zu machen.

Während es für die Funktionalität eines IT-Systems eine definierte und überprüfbare Anforderungsliste gibt, lässt sich eine solche für die IT-Sicherheit nicht erschöpfend erstellen. Denn es gibt unendlich viele denkbare Szenarien, die das System beeinträchtigen könnten - vom Anwenderfehler bis hin zum gezielten Angriff. Hinzu kommt: Cyberkriminelle entwickeln ihre Angriffsmethoden ständig weiter. Um bei der IT-Sicherheit die gleiche Gewissheit zu haben wie bei der Funktionalität, müsste ungleich mehr Zeit und Geld in das Härten des Systems als in dessen Entwicklung gesteckt werden. Trotzdem ist eine abschließende Prüfung auf Sicherheit unmöglich.

Security von Beginn an mitdenken

Um die Kosten im Griff zu behalten und das geforderte Sicherheitsniveau zu gewährleisten, bedarf es einer grundlegend anderen Herangehensweise an die IT-Sicherheit. Statt sich zunächst nur auf die Funktionalität von Systemen, Lösungen und Infrastrukturen zu konzentrieren und dann zu versuchen, Sicherheit nachträglich zu integrieren, muss die Security von Beginn an elementarer Bestandteil der Produkt- und Lösungsentwicklung sein. Sie ist keine Produkteigenschaft, sondern ein Entwicklungsziel - meist als Security by Design bezeichnet. Statt also erst überall Türen zu verbauen und anschließend ein Brandschutzkonzept umzusetzen, muss erst das Brandschutzkonzept stehen. Notwendige Türen sollten dann Teil dieses Konzepts sein.

Ein weiteres Ziel ist Security by Default, also sicher vorkonfigurierte Lösungen out of the box. Nur mit diesen beiden Prinzipien lassen sich echte Sicherheitsfortschritte in IT-Infrastrukturen erzielen.

Technik allein löst das Problem allerdings nicht. Eine wesentliche Voraussetzung für bessere Sicherheitssysteme ist die Firmenkultur: Diese muss darauf ausgerichtet sein, Security by Design und Security by Default nachhaltig umzusetzen. Dies gilt für alle Unternehmen in der Lieferkette, denn der Endkunde allein kann keine umfassende Sicherheit gewährleisten. Zudem setzt nachhaltige Sicherheit ein proaktives Herangehen voraus. Reaktive Lösungen mit immer neuen Patches helfen wenig, da bis zum Einspielen dieser Flicken reale Sicherheitslücken existieren - und das, wie die Praxis zeigt, oft über Tage, Wochen oder gar Monate.

Sicherheit von Grund auf:
Security by Design, Security by Default und Zero Trust sind gelebte Firmen-DNA von IT-Security-Spezialist genua. Produkte wie die Central Management Station genucenter und Fernwartungslösung genubox erfüllen höchste Sicherheitsstandards.

(Quelle: genua GmbH)

Auch führt das Patchen zu Störungen der Betriebsabläufe und zu Ausfallzeiten. Insbesondere nicht homogene Systeme, die nachträglich gehärtet wurden, sind davon betroffen. Denn Entwicklung und Sicherung solcher Systeme erfolgen nicht aus einer Hand. Am Ende sind diese Systeme bestmöglich nach außen geschützt, aber niemand weiß, ob nicht in einer Subroutine potenziell maliziöser Code schlummert, der ohne Patch und Update jahrelang läuft und plötzlich zu einem Problem werden kann - Stichwort Log4j. Hier ist nicht Open-Source-Software das Problem, sondern Entwicklungspraktiken, die eher auf schnelle Ergebnisse als auf nachhaltige Wartbarkeit und Sicherheit ausgerichtet sind.

Einen proaktiven Ansatz wählen

Security by Design fördert einen proaktiven Ansatz für die IT-Sicherheit, in dem von Anfang an Schutzmaßnahmen gegen potenzielle Bedrohungen aufgebaut werden, anstatt erst nach deren Auftreten darauf zu reagieren. Sicherheitsbedrohungen werden frühzeitig im Entwurfsprozess antizipiert und entschärft, was Unternehmen erhebliche Kosten im Zusammenhang mit Sicherheitsvorfällen sparen kann. Systeme, die nach den Grundsätzen von Security by Design entwickelt wurden, genießen zudem oft größeres Vertrauen bei Anwendern und Kunden.

Aber auch bei einer durchdachten Sicherheitsarchitektur gibt es keine hundertprozentige Sicherheit. Deswegen muss neben der Prävention auch dafür Sorge getragen werden, dass ein erfolgreicher Angriff nur minimalen Schaden anrichten kann. Mehrschichtige Sicherheitskonzepte, bei denen verschiedene Ebenen mit automatisierten Funktionen zum Erkennen und Abwehren von Angriffen (Detection and Response) abgesichert sind, können potenzielle Schäden drastisch reduzieren

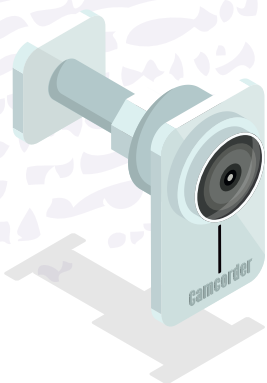
und sind daher ebenso Teil der Architektur wie leistungsfähige Recovery-Funktionen. Denn am Ende gilt der Grundsatz: Egal, was man an wen delegiert - den Schaden hat man selbst.

Zero Trust: Vertrauen ins Misstrauen

Das Reduzieren der Komplexität eines Systems ist ein wichtiger Schlüssel, um das höchstmögliche Maß an Security zu erlangen. Gleichzeitig ist genau das unglaublich schwierig, eben weil die Umgebungen so komplex sind und viele meist dynamische Anforderungen erfüllen müssen.

Anstatt eine bestehende Lösung ständig zu erweitern, ist es sinnvoller, sie in einfache Module zu zerlegen - oder zumindest in Komponenten mit einfachen, klar definierten Schnittstellen. Das Zusammenspiel dieser Komponenten über diese Schnittstellen muss leicht zu beschreiben, einzuschränken und kontrollierbar sein. Wie bei Anwendern sollte man das Prinzip der geringsten Rechte umsetzen. Die separierten, robusten Komponenten dürfen sich zudem nicht negativ beeinflussen können. Eine solche Separation führt zu mehr Robustheit gegenüber potenziellen Bugs, menschlichen Fehlern und Angriffen und hilft, das Schadenspotential zu verringern.

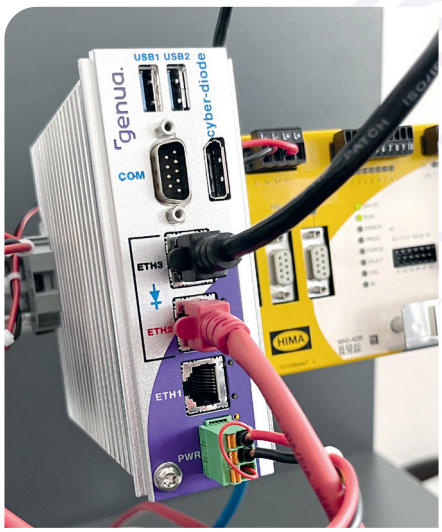
Security by Design setzt grundsätzlich eine Zero-Trust-Mentalität voraus, die in der Unternehmenskultur verankert sein muss. Das bedeutet, dass man nicht einmal dem eigenen Code vollständig vertrauen sollte, geschweige denn dem von Zulieferern.



Defense in Depth

Heutige Systeme und Netzwerke sind sehr komplex und dadurch fehleranfällig. Wirklich zu schützen sind sie nur durch mehrschichtige Sicherheitsmaßnahmen, die sich gegenseitig unterstützen, um bei Fehlern angemessen reagieren zu können (Defense in Depth). Ein solcher Multilayer-Ansatz sollte sowohl im Code als auch in der Infrastruktur verfolgt werden.

Darüber hinaus sind Penetration-Tests wichtig, um die Widerstandsfähigkeit gegen typische Angriffe zu testen und gezielte Härtungen vorzunehmen. Wobei klar sein muss, dass sich Security nicht in



Richtungsweisend: **Die cyber-diode von genua sendet Daten per OPC UA sicher aus einer Sicherheitssteuerung (hier: HIMatrix) an eine Cloud-Anwendung, um Prüfzyklen für Geräte und Steuerungen zu berechnen.**

ein System „hineintesten" lässt. Unabhängige Audits durch Experten und darauf aufbauende Zertifizierungen sind ein weiterer Baustein für vertrauenswürdige Sicherheit. Defense in Depth ist grundlegender Bestandteil von und damit Voraussetzung für Security by Design.

Zusätzlich zum Härten der Angriffsfläche mit Defense in Depth gilt es, auch die Größe der Angriffsfläche und den möglichen Schaden klein zu halten. Bei der eingehenden Kommunikation von extern helfen Perimeter-Firewalls, die auch ausgehende Kommunikation nach extern analysieren und filtern. Dadurch lässt sich bei einer erfolgreichen Kompromittierung die Steuerung durch den Angreifer und das Nachladen von Schadcode unterbinden. Laterale Bewegung von Angreifern, die den Perimeter bereits überwunden haben, lässt sich durch Mikrosegmentierung begrenzen. In einer solchen Situation zeigt sich dann die Stärke von Defense in Depth, da der Angreifer es zwar ins Netz geschafft hat, dort aber seine Ziele wie die Ausweitung von Zugriffsrechten nicht erreicht. Deshalb ist es wichtig, sich nie auf einzelne Schutzmechanismen zu verlassen.

Mehr Planungssicherheit durch Security by Design

Security by Design sorgt für eine bessere Planungssicherheit, denn es kann ungeplante Produktionsunterbrechungen aufgrund erfolgreicher Angriffe oder dem erforderlichen unverzüglichen Aufspielen von Not-Patches vermeiden. Auch der Personalbedarf lässt sich besser planen. Damit kann Security by Design dazu beitragen, die Gesamtkosten zu senken.

Komponenten wie das Netzmanagement oder Endpoint-Sicherheit sowie Firewalls müssen tief in das System eingreifen können und benötigen ihrerseits umfassende Zugriffsrechte. Bei falscher Auslegung oder Konfiguration können solche Lösungen schnell selbst zu Gefahrenherden werden – wie aktuelle Beispiele ausgenutzter Zero-Day-Sicherheitslücken zeigen. Daher sollten hier nur Systeme zum Einsatz kommen, die mit Security by Design und Security by Default entwickelt wurden.

Thomas Hertel – Fachjournalist
www.genua.de

Akte xz-Backdoor

CYBERSICHERHEIT IN DER SOFTWARE SUPPLY CHAIN

Der Vorfall um die Open-Source-Kompressionsbibliothek xz, die über Ostern große Teile des Internets zu beeinträchtigten drohte, wirft Fragen zur sicheren Nutzung von Open-Source-Software auf. Was bringt in diesem Zusammenhang der neue Cyber Resilience Act, der Hersteller von Produkten mit digitalen Elementen zu mehr Cybersicherheit über den gesamten Produktlebenszyklus verpflichtet? Alexander Bluhm und Steffen Ullrich, genua, erklären im Gespräch mit it management, wie die Open-Source-Welt funktioniert und wie Produkte trotz möglicher Fehler sicher genutzt werden können.

it management: *Wie kann es sein, dass auch in moderner Software immer wieder Fehler auftauchen, die Anwender massiv in die Bredouille bringen können?*

Alexander Bluhm: Bei digitalen oder smarten Gütern ist Software das bestimmende Element. Sie ist heutzutage meistens nicht mehr aus einer Hand. Vielmehr handelt es sich oft um eine Komposition aus Hunderten oder Tausenden von Modulen, die teilweise oder sogar größtenteils aus öffentlichen Open-Source-Bibliotheken stammen. Das ist durchaus sinnvoll. Funktionen wiederholen sich – und warum sollte man das Rad jedes Mal neu erfinden? Im Laufe mehrerer Jahrzehnte haben sich Open-Source-Bibliotheken gut gefüllt – es gibt kaum eine Funktion, die man dort nicht findet. Gerade KMU mit knappen Budgets sind bei ihrer Softwareentwicklung stark auf die Verfügbarkeit freier Open-Source-Module angewiesen.

it management: *Das ist nachvollziehbar. Und wo genau entsteht das Problem?*

Alexander Bluhm: Die Herausforderung liegt darin, die Qualität der Open-Source-Module, die eventuell in eigenen Software-Projekten zum Einsatz kommen sollen, richtig zu beurteilen. Die Open-Source-Community ist keine homogene Gruppe. Oft sind es stark engagierte Menschen, die Projekte ohne finanzielles Kalkül in ihrer Freizeit vorantreiben. Viele sind echte Profis, andere starten vielleicht gerade ihre ersten Programmierversuche. Daneben gibt es auch langjährige Projekte, die von großen Firmen unterstützt werden und bei dem die Entwickler in feste Arbeitsverhältnisse übernommen wurden. Entsprechend unterschiedlich sind die Qualitätsstandards. Es ist Aufgabe desjenigen, der die Software einsetzt oder weiter vertreibt, den Unterschied zu erkennen.

> DIE HERAUSFORDERUNG LIEGT DARIN, DIE QUALITÄT DER OPEN-SOURCE-MODULE, DIE EVENTUELL IN EIGENEN SOFTWARE-PROJEKTEN ZUM EINSATZ KOMMEN SOLLEN, RICHTIG ZU BEURTEILEN.
>
> **Alexander Bluhm,**
> **IT-Sicherheitsexperte, genua GmbH, www.genua.de**

it management: *Gibt es bei Open Source keine Standardprozesse um die Software zu überprüfen?*

Alexander Bluhm: Nein, die Verantwortung für die Sicherheit der Open-Source-Module und deren korrekter Integration liegt bei dem Unternehmen, das sie für seine kommerzielle Software nutzt. Auf welche Weise diese Verantwortung wahrgenommen wird, hängt unter anderem von der Kompetenz der verfügbaren Fachkräfte und der bereitgestellten Zeit zur Prüfung ab, aber auch von der Bedeutung der eingesetzten Open-Source-Komponente für das Produkt.

it management: *Kürzlich sorgte eine Backdoor in der Open-Source-Bibliothek xz für Aufsehen, weil sie das gesamte Internet hätte beeinträchtigen können. Wie sehen Sie das?*

Alexander Bluhm: Der Fall war extrem kritisch und hätte drastische Auswirkungen auf die Zuverlässigkeit des Internets haben können. Er zeigt die Schwachstellen eines vermeintlich unkritischen Einsatzes von Fremdsoftware und wie kleine Projekte große Auswirkungen haben können. Die xz ist auf vielen weltweit genutzten Linux-Systemen eng mit dem SSH-Zugang verbunden, wodurch ein kleiner Fehler immense Bedeutung erlangt. Über SSH werden Server administriert, einschließlich der in medizinischen und anderen smarten Geräten. Eine SSH-Hintertür, die beliebige Befehle ausführt, hätte verheerende Folgen.

it management: *Wie konnte das passieren?*

Steffen Ullrich: Das kleine Open-Source-Projekt xz wurde jahrelang von einem einzelnen Freiwilligen betreut. Als er über Burn-out klagte, bot ein Unbekannter, der sich Jia Tan nennt, seine Hilfe an und erschlich sich sein Vertrauen. Dies wurde gefördert durch Mails „ungeduldiger" Nutzer, was eventuell eine koordinierte Aktion mit weiteren Cyberkriminellen war. Schließlich wurde Jia Tan Co-Betreuer mit dem Recht, eigenen Code einzubringen. Dieses Recht missbrauchte er für den Einbau einer nahezu unsichtbaren Hintertür. Nur durch Zufall ist diese Backdoor bei der Analyse eines Performanceproblems aufgefallen.

it management: *Was tun Software-Hersteller und Gesetzgeber, um die Qualitätsstandards bei Software zu verbessern? Kann der kürzlich beschlossene Cyber Resilience Act (CRA) hier Positives bewirken?*

Steffen Ullrich: Der Cyber Resilience Act (CRA) strebt eine umfassende Verbesserung der Software-Lieferkette an. Er gilt für alle digitalen Produkte, einschließlich Software, Hardware und Cloud-Lösungen, und führt „Security by Design" in das europäische Recht ein. Risiken und Cybersicherheitsmaßnahmen müssen jetzt kontinuierlich über den gesamten Produktlebenszyklus bewertet werden. Hersteller müssen sichere Entwicklungsprozesse etablieren, Cybersicherheitsrisiken dokumentieren und Schwachstellen aktiv melden und beheben. Der CRA betrifft die gesamte Wertschöpfungskette, von Herstellern über Distributoren bis hin zu Importeuren.

it management: *Inwieweit betreffen diese Vorgaben Open Source?*

Steffen Ullrich: Für Open Source gibt es Ausnahmen, um das Open-Source-Ökosystem nicht zu belasten und Freiwillige vor untragbaren Haftungsrisiken zu schützen. Diese Ausnahmen gelten aber nur für Entwickler sowie für als „Open-Source Software Stewards" agierende Organisationen, nicht für Unternehmen, die Open-Source-Komponenten nutzen. Der CRA ergänzt im Rahmen der EU-Cybersicherheitsstrategie 2020 zum Beispiel NIS-2 und stärkt die Sicherheit in der Software-Lieferkette.

it management: *Wie können Endkunden die Sorgfalt von Unternehmen beurteilen, um beim Kauf kein Cybersicherheitsrisiko einzugehen?*

Steffen Ullrich: Wer mit einem Produkt Geld verdient, muss auch für dessen Sicherheit sorgen. Der CRA greift folgende zwei Probleme auf: Erstens das unzureichende Maß an Cybersicherheit vieler Produkte, zweitens die Unfähigkeit von Verbrauchern und Unternehmen zur richtigen Beurteilung der Produkte oder zu deren sicheren Betrieb. Unternehmen müssen mehr Mittel für Tests und Sicherheitsprozesse aufbringen. Anhand von sichtbaren Kriterien sollen Kunden prüfen können, dass der Hersteller die von ihnen benötigten Sicherheitsstandards einhält.

it management: *Können Sie das ein wenig ausführen?*

Steffen Ullrich: Unternehmen können viel für die Sicherheit tun, etwa durch den

> DURCH BEWUSSTE EINSCHRÄNKUNG AUF NÜTZLICHE FUNKTIONEN LÄSST SICH DIE KOMPLEXITÄT EINER SOFTWARE REDUZIEREN – UND DAMIT DIE ANZAHL VON SICHERHEITSLÜCKEN.
>
> **Steffen Ullrich, IT-Sicherheitsforscher, genua GmbH, www.genua.de**

Aufbau einer umfassenden Sicherheitskultur. Beispiele wie Microsoft oder Cisco zeigen, dass dies Zeit braucht. In Deutschland ist die Zusammenarbeit von Herstellern mit dem Bundesamt für Sicherheit in der Informationstechnik samt entsprechender Zertifikate und Zulassungen ein guter Indikator für hohe Ansprüche an die Cybersicherheit ihrer Produkte und die Qualität der Entwicklungsprozesse. Für Unternehmen mit hochwertig zertifizierten Produkten ist „Security by Design" längst gelebte Praxis.

Ein weiterer Punkt ist die bewusste Einschränkung auf nützliche Funktionen, um die Komplexität und damit Sicherheitslücken zu reduzieren. Fremdsoftware sollte restriktiv, etwa in einer Sandbox, eingebunden werden. Wichtige Sicherheitsstrategien sind Defense-in-Depth, Separation und Segmentierung.

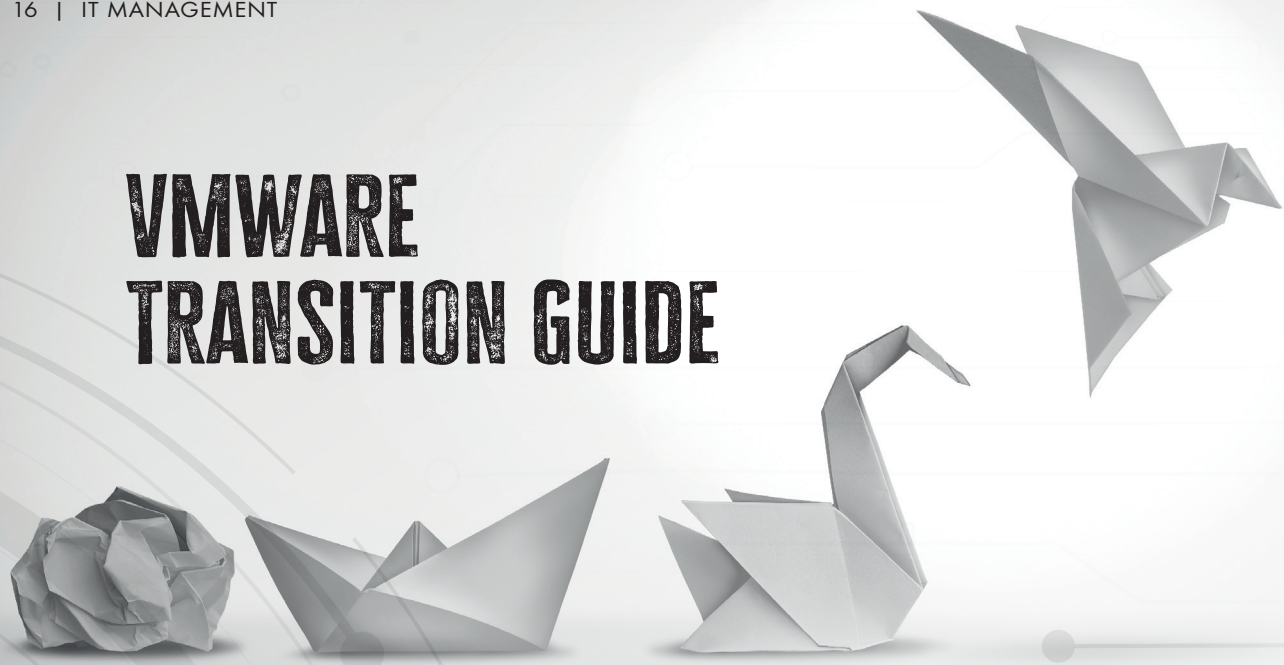
? **it management:** *Würden Sie, trotz der Bedenken bezüglich der Sicherheit und Zuverlässigkeit, den Einsatz von Open Source-Software auch weiterhin empfehlen?*

Alexander Bluhm: Auf jeden Fall! Man darf nicht vergessen: Kommerzielle Software hat zwar andere Probleme, aber die gleichen Risiken! Ich verwende ausschließlich Open-Source, nicht einsehbare Software ist mir suspekt und nicht nachvollziehbar.

! **it management:** *Herr Bluhm, Herr Ullrich, vielen Dank für das Gespräch!*

THANK YOU

VMWARE TRANSITION GUIDE



ZUR STÄRKUNG IHRER VIRTUALISIERUNGSSTRATEGIE IN ZEITEN DES WANDELS

In der dynamischen IT-Welt, in der Fortschritt und Umbruch Hand in Hand gehen, ist Veränderung die einzige Konstante. VMware hat sein Produktangebot, seine Lizenzmodelle und seine Verträge mit Partnern einer Reihe umfassender Änderungen unterzogen. Diese sind eine direkte Folge der Übernahme durch Broadcom im November 2023 und der Ausgangspunkt nachwirkender Umstellungen in der VMware Technologiewelt.

Allerdings ist auch jede Änderung gleichzeitig eine neue Chance. Somit ist jetzt für VMware-Kunden und -Partner ein günstiger Moment, ihre Virtualisierungsstrategie noch einmal zu überdenken. Angesichts des Ausmaßes der Umstellungen sollte man als erstes herausfinden, was das konkret für Ihren Geschäftsbetrieb und Ihre Zukunftsplanung bedeutet.

Dieser Leitfaden bietet Ihnen einen Überblick zu den wesentlichen Änderungen und strategischen Alternativen.

Inhalt des eBooks:

- #1 Wie Sie die Folgen der Übernahme durch Broadcom meistern
- #2 Umstellungen in der Lizenzierung, die die VMware-Landschaft auf den Kopf stellen
- #3 Diese Fragen sollten Sie sich stellen
- #4 Für VMware optimierter Speicher, der zudem einen nahtlosen Wechsel ermöglicht
- #5 Unterbrechungsfreie Ablösung von VMware vSAN mit SANsymphony
- #6 Auswahl über VMware vSphere hinaus ermöglichen
- #7 Maximale VMware-Effizienz mit SANsymphony

Das **eBook** umfasst 11 Seiten und steht zum kostenlosen Download bereit

EFFIZIENZ, TRANSPARENZ UND COMPLIANCE

Getrieben durch technologische Innovationen und wachsende Anforderungen, befindet sich die Finanzbranche mehr denn je in einem stetigen Wandel.

Intelligente Automatisierungslösungen revolutionieren die Art und Weise, wie finanzielle Prozesse gesteuert und Daten verarbeitet werden. Zugleich gewinnen Themen wie Integrität und ethische Grundsätze zunehmend an Bedeutung für vertrauenswürdige Finanzdienstleistungen. Darüber hinaus eröffnet der Einsatz von Künstlicher Intelligenz völlig neue Möglichkeiten, um komplexe Finanzanalysen zu beschleunigen und Entscheidungen datenbasiert zu optimieren.

KI im Rechnungswesen

INNOVATIONEN UND HERAUSFORDERUNGEN

Je „intelligenter" eine Software, desto eher ist sie in der Lage, Menschen manuellen Arbeitsaufwand abzunehmen. Bezogen auf das Rechnungswesen heißt das zum Beispiel, die täglichen Arbeitsprozesse mit einem Rechnungsworkflow zu optimieren, der KI und maschinelles Lernen nutzt. Mit diesen Technologien werden schnellere Datenverarbeitung, präzisere Analysen und verbesserte Entscheidungsfindungen erreicht.

Es sind die klassischen Routineaufgaben, die sonst ein Mensch manuell ausführen muss: Transaktionen kategorisieren, Rechnungen verarbeiten, Zahlungen überwachen und Berichte generieren. Der Einsatz maschinellen Lernens und hochentwickelter Algorithmen ermöglicht eine weitere Automatisierung solcher Buchhaltungs- und Finanzprozesse. Resultat sind Einsparung von Zeit und Ressourcen, Entlastung für die Beschäftigten, eine schnellere Datenverarbeitung, präzisere Analysen durch genaue, konsistente Finanzdaten und dadurch fundierte Entscheidungen.

Drei Beispiele, wie KI-Algorithmen heute in der Praxis bereits unterstützen:

#1 Selbstlernende Datenextraktion

Bei der Beleglesung lernt die Software mit. Aus den Änderungen, die in der Validierung vorgenommen werden, übernimmt sie die Informationen – ohne dass die Beleglesung noch einmal explizit trainiert werden muss.

#2 Intelligente Kontierungsvorschläge

Welche Kontierung für eine Rechnung in Frage kommt, lässt sich meist nicht durch Regelwerke eindeutig abbilden. Man muss den Kontext kennen und daraus die Kontierung ableiten. Mit Hilfe von Künstlicher Intelligenz lassen sich Kontierungsvorschläge inklusive Wahrscheinlichkeit erstellen, aus denen die Beschäftigten nur noch auswählen müssen.

DIE VORTEILE VON KI IM RECHNUNGSWESEN IN ANSPRUCH NEHMEN BEDEUTET GLEICHZEITIG, SICH DER DAMIT VERBUNDENEN HERAUSFORDERUNGEN BEWUSST ZU WERDEN.

Anne Teterra,
Product Manager, xSuite Group GmbH,
www.xsuite.com

#3 Vorschlagsfunktion für die Bearbeiterfindung

In Unternehmen mit über die Jahre gewachsenen Strukturen und weniger gut dokumentierten Prozessen und Verantwortlichkeiten ist es relativ aufwändig, im System zu hinterlegen, welcher Mitarbeitende unter welchen Bedingungen für welche Belege und Arbeitsschritte zuständig ist. Hier kann KI Aufwand einsparen, denn die Regeln zur Bearbeiterfindung sind oft so aufgebaut, dass eine Rechnung zur Prüfung bei einer Gruppe von Personen ankommt und der richtige Bearbeitende automatisch bereits in der Validierung vorgeschlagen wird.

Prognosen und Analysen

KI-basierte Analysetools ermöglichen es des Weiteren, große Mengen an Daten sinnvoll auswerten zu können. Sie spielen eine entscheidende Rolle bei der Erstellung präziser Prognosen und Vorhersagen, indem sie aus der Datenanalyse heraus Trends, Muster und Risiken identifizieren. Die Nutzung dieser Erkenntnisse ermöglicht es Unternehmen, ihre finanzielle Leistung zu verbessern, Kosten zu senken und Chancen für Wachstum und Expansion zu erkennen. Hier liegen noch große Potenziale, die es zu heben gilt. Das Voranschreiten der Digitalisierung ist eine Notwendigkeit, um diese Daten nutzbar zu machen.

Risikomanagement und Compliance

Indem sie mit Hilfe von KI-Technologien Risiken frühzeitig identifizieren und bewerten können, sichern Unternehmen ihre finanzielle Stabilität, denn so können sie auch präventive Maßnahmen ergreifen. KI-basierte Systeme unterstützen zudem darin, Compliance-Vorschriften einzuhalten, indem sie Transaktionen überwachen und auf Unregelmäßigkeiten hinweisen – sind sie doch sozusagen Meister im Erkennen von Abweichungen in Mustern – sie haben einen „Blick" für Anomalien.

Einsatz mit Augenmaß

Die Vorteile von KI im Rechnungswesen in Anspruch nehmen bedeutet gleichzeitig, sich der damit verbundenen Herausforderungen bewusst zu werden. Datenschutzbedenken gehören dazu, ebenso wie die Notwendigkeit, Mitarbeitende zu finden, die qualifiziert damit umgehen können. Die neuen Technologien müssen außerdem in bestehende Systeme integriert

werden und das Unternehmen muss die Genauigkeit und Zuverlässigkeit von KI-gestützten Analysen gewährleisten können. Auch die Rollenbilder der eigenen Beschäftigten befinden sich dabei im Wandel und die Anforderungen an diese werden sich ändern.

Die Bedeutung von KI im Rechnungswesen wird voraussichtlich weiter zunehmen, da Unternehmen bestrebt sind, ihre Finanzprozesse zu optimieren und Wettbewerbsvorteile zu erlangen. Fachabteilungen müssen hier als Treiber der Digitalisierung fungieren, um Transparenz und Effizienz zu steigern.

Nicht immer passt es

Auch bei der Eingangsrechnungsverarbeitung gibt es mehr oder weniger geeignete Einsatzszenarien von KI. Zum Beispiel bei der Feststellung der Belegart: Die Entscheidung, ob es sich um eine FI- oder MM-Rechnung handelt, lässt sich auf eine einzelne Ja-/Nein-Frage herunterbrechen: „Ist eine Bestellnummer auf der Rechnung vorhanden?" Diese Aufgabe ist damit perfekt für ein fest hinterlegtes Regelwerk geeignet, KI an dieser Stelle einzusetzen wäre unsinnig.

Ein anderes Beispiel ist die Bearbeiterfindung, die in Bezug auf die Rechnungsfreigabe auch rechtliche Aspekte hat. Diese kann in hinterlegten Regelwerken klar definiert und abgeleitet werden. Eine KI kann hier nicht immer eine 100prozentige Sicherheit bieten. Daher gilt es abzuwägen, ob hier eine Vollautomatisierung durch KI-Algorithmen möglich ist.

So viel steht fest: Unternehmen sind bestrebt, ihre Finanzprozesse zu optimieren und Wettbewerbsvorteile zu erlangen. Die Bedeutung von KI im Rechnungswesen wird vor diesem Hintergrund mit Sicherheit weiter zunehmen. Durch ihre kontinuierliche Weiterentwicklung und Anpassung an neue Technologien können Unternehmen ihre Vorteile voll ausschöpfen und sich erfolgreich in einer zunehmend digitalen Wirtschaft positionieren.

KI braucht die Public Cloud

Künstliche Intelligenz braucht Daten als Lernmenge. In einer Public-Cloud-Lösung liegen diese in ungleich größerer Anzahl als bei einzelnen, on-premises installierten Systemen vor. Zudem gibt es aus der Cloud bereits Lösungen, auf die man sinnvollerweise zugreifen kann.

Der Einsatz von KI ist deshalb eng verbunden mit der zunehmenden Nutzung von Public-Cloud-Angeboten. Dieses Prinzip verfolgt auch die xSuite, in dem sie digitale Workflows aus der Cloud unter Einsatz von KI zur Vereinfachung und Automatisierung von Abläufen bereitstellt wie ihren Eingangsrechnungsworkflow auf der SAP Business Technology Platform. Mittelfristig werden SaaS- und Public-Cloud-Lösungen wie diese deshalb zum führenden Standard bei digitalen Geschäftsprozessen werden.

Anne Teterra

Bild: iStock

Consolidation & Financial Analytics

FINANZ-AUTOMATION-SOFTWARE ALS BINDEGLIED ZUM ERP

Die Finanzorganisation eines Unternehmens ist mit einem Fachwerkhaus vergleichbar. Die Qualität der einzelnen Elemente ist enorm wichtig, aber das stabile Tragwerk ist erst dann gegeben, wenn die Balken, Spanten, Stützen und Verbindungen zuverlässig miteinander verbunden sind und die Statik ausgewogen auf den Fundamenten ruht.

Wie bei einem Gebäude basiert das moderne Finance & Accounting (F&A) auf folgenden Grundpfeilern: dem Invoice-to-Cash, Procure to Pay, dem Finanzabschluss, den Intercompany-Bewegungen sowie dem Consolidation & Financial Analytics. All diese Bereiche werden durch ERP oder spezielle Finance & Accounting-IT-Lösungen unterstützt und sollten engverzahnt mit möglichst vielen automatisierten Prozessen aufeinander aufbauen, um die Grundlage für eine effiziente und wirtschaftliche Steuerung des Unternehmens zu bilden.

Der Bereich Consolidation & Financial Analytics nimmt in der Finanzorganisation und im Controlling allerdings eine besondere Rolle ein. Denn hier werden die Finanzdaten vor allem für die externe Kommunikation aufbereitet. Deshalb müssen diese Zahlen und Analysen akkurat, schnell sowie hoch aktuell zur Verfügung stehen.

Tradition muss der Moderne weichen

Mit der Schlüsselfunktion der Consolidation & Financial Analytics haben einige Unternehmen jedoch eine Herausforderung. Denn die Konsolidierung der Einzelabschlüsse findet unter hohem Zeitdruck statt. Erschwerend kommt hinzu, dass die schnellen Märkte die Unternehmen immer mehr dazu zwingen, agil zu handeln – was eine rasche oder gar kontinuierliche Kommunikation und Berichterstattung, beispielsweise gegenüber Banken, Investoren oder Aktionären, einschließt.

DEM PROBLEM DER QUELLENVIELFALT UND DER POTENZIELLEN UNVOLLSTÄNDIGKEIT DER INFORMATIONEN, KANN MIT EINER GEZIELTEN AUTOMATISIERUNG ENTGEGENGEWIRKT WERDEN.

Ralph Weiss,
Geo VP DACH, BlackLine,
www.blackline.com

Um Consolidation & Financial Analytics zu realisieren, muss eine Vielzahl an Dokumenten, Reports und Tabellen aus unterschiedlichen Quellen zusammengeführt werden. Oft erfolgen diese Prozesse noch manuell, aufwendig und risikobehaftet. Und trotzdem sollen die Finanzexperten nach dem Zusammentragen der Einzelinformationen in der Lage sein, aussagekräftige Analysen aus den Daten zu ziehen, damit das Management und die Stakeholder die richtigen Entscheidungen zum Wohle des Unternehmens treffen können. Das ist, als ob man aus teils ungeprüftem Baumaterial ein Haus zimmert und hofft, dass es dem nächsten Windstoß standhält.

Diesen Zustand bestätigten die Daten einer aktuellen Marktforschung: In einer Studie, die Censuswide im Auftrag von BlackLine weltweit unter 1.339 C-Level und Finanzprofis durchgeführt hat, sagen 55 Prozent, dass sie nicht ganz sicher sind, ob sie finanzielle Fehler vor der Meldung der Ergebnisse erkennen können. Auf die Frage, warum sie den Daten ihres Unternehmens nicht voll vertrauen, antwortete weltweit fast ein Drittel (26 Prozent der deutschen Befragten), dass die Daten aus zu vielen verschiedenen Quellen stammen, sodass sie nicht sicher sein können, dass alle Daten berücksichtigt werden. Weitere Gründe sind die Abhängigkeit von umständlichen Tabellenkalkulationen, welche die F&A-Teams bis zum Monatsende im Dunkeln tappen lassen (27 Prozent insgesamt / 22 Prozent in Deutschland) und veraltete Prozesse - einschließlich der manuellen Datenerfassung, die anfällig für menschliche Fehler ist (25 Prozent insgesamt / 22 Prozent in Deutschland).

Was also braucht der Hausherr, wenn er schnelle Ergebnisse benötigt und dabei sicher sein will, dass das Resultat höchsten Ansprüchen genügt? Er benötigt Standards, Geschwindigkeit und Risikoredu-

zierung. Und diese Ziele erreicht er mit IT-gestützten Finanzprozessen, die zu einem hohen Grad automatisiert sind. Dies gilt für alle Bereiche der Finanzorganisation, denn erst wenn die einzelnen Vorprozesse, die Geschwindigkeit und die Qualität von der Grundstruktur bis zum Dachgeschoss auf höchstem Niveau ausgeführt werden, kann der Giebel gesetzt werden, der bildlich der Consolidation & Financial Analytics gleichkommt.

Finanzautomation ist ein Muss

In der bereits erwähnten Studie und bei der Frage, was Unternehmen helfen würde, beispielsweise bei disruptiven Situationen agil zu bleiben, nennen über 20 Prozent der Befragten Finanzprofis die Fähigkeit, komplexe Finanzinformationen an verschiedene Interessengruppen und Stakeholder zu vermitteln. Ebenso viele nennen die Fähigkeit, die Finanzdaten zu verstehen und zu analysieren. In diesem Zusammenhang ist es wenig verwunderlich, dass über 20 Prozent der Befragten der Meinung sind, dass nicht genügend automatisierte Kontrollen und Überprüfungen für das Datenvolumen existieren.

Eine Lösung dieser Probleme ist nicht nur in Sicht, sie existiert. Dem Problem der Quellenvielfalt, der potenziellen Unvollständigkeit der Informationen und des Fehlerrisikos bei der Zusammenführung der Finanzdaten, kann mit einer gezielten Automatisierung entgegengewirkt werden. Für die Consolidation & Financial Analytics ist dies von entscheidender Bedeutung, denn wenn bereits an der Basis der Finanzorganisation auf ein Höchstmaß an Automatisierung gesetzt wird, stehen der Consolidation & Financial Analytics jederzeit valide Daten zur Verfügung. Mehr noch: Wenn die Automatisierungsprozesse zudem kontinuierlich ablaufen, anstatt zu Monats- oder Quartalsende, nachdem die Einzelabschlüsse an das Konsolidierungssystem übermittelt werden, stehen für die Consolidation & Financial Analytics Echtzeitdaten zu jedem Zeitpunkt unterperiodisch zur Verfügung. Und genau das versetzt ein Unternehmen und seine Stakeholder in die Lage, das Unternehmen agil, zielgerichtet und sicher zu lenken.

Doch Automatisierung ist nicht gleich Automatisierung. In der Vergangenheit hat sich gezeigt, dass viele Unternehmen auf Robotik oder Automatisierung – sogar unter Einsatz Künstlicher Intelligenz – gesetzt haben. Dieser Ansatz ist grundsätzlich zu begrüßen, hat aber einen systemimmanenten Fehler, wenn nicht übergreifend automatisiert wird, sondern nur an einzelnen Stellen. Eine lückenhafte Automatisierung mit Insellösungen hat zur Folge, dass Unternehmen mit einer zunehmend heterogenen Lösungsvielfalt zu kämpfen haben. Mit einem derartigen Flickenteppich aus einzelnen Automatisierungslösungen lassen sich zwar in Teilbereichen Verbesserungen erzielen, aber die Vorzüge eines ganzheitlichen Digitalisierungskonzepts, wie es für die Consolidation & Financial Analytics vonnöten ist, kann so nicht entstehen.

Damit die Automatisierung aller Prozesse im Finance & Accounting nicht zur unüberschaubaren Mammutaufgabe avanciert, existieren Lösungen für die Finanzautomation - beispielsweise von BlackLine. Sie arbeiten nahtlos mit allen klassischen ERP- und Finanzlösungen zusammen und standardisieren und automatisieren die Prozesse eines Ökosystems auf einem Höchstmaß. Mehr noch: Spezielle Lösungen wie die BlackLine Financial Reporting Analytics bauen auf die automatisierten Prozesse der Finanzorganisation auf und ermöglichen dem CFO eine nahtlose On-Demand-Analyse von Einzelposten und Abweichungen auf Konzernebene mit effizienter, durchgängiger Transparenz und Nachvollziehbarkeit.

So funktioniert Finance & Accounting heute – modern, standardisiert und automatisiert für höchste Effizienz.

Ralph Weiss

Integrität in der Finanzbranche

PAPIERBASIERTE WIRTSCHAFTSPRÜFUNGSVERFAHREN GEHÖREN DER VERGANGENHEIT AN

In einer Zeit, in der die Dynamik und Komplexität des Finanzsektors neue Herausforderungen birgt und das Risiko für Finanzbetrug weiter wächst, rücken fortschrittliche Verifizierungsverfahren in den Vordergrund, um die Zuverlässigkeit und Sicherheit der Finanzberichterstattung zu gewährleisten.

Laut einer Studie des Instituts der deutschen Wirtschaft (IW) vom April 2024 ist die Anzahl der von Wirtschaftskriminalität betroffenen Unternehmen so hoch wie seit 2014 nicht mehr: Mehr als jedes dritte Unternehmen ist von wirtschaftskriminellen Handlungen betroffen, mit steigender Tendenz. Die Raffinesse der Betrugsversuche nimmt stetig zu. In diesem Zusammenhang sind Finanzverantwortliche gezwungen, ihre Präventionsstrategien zu verstärken und digital aufzurüsten.

Proaktivität als Schlüssel zur Betrugsprävention

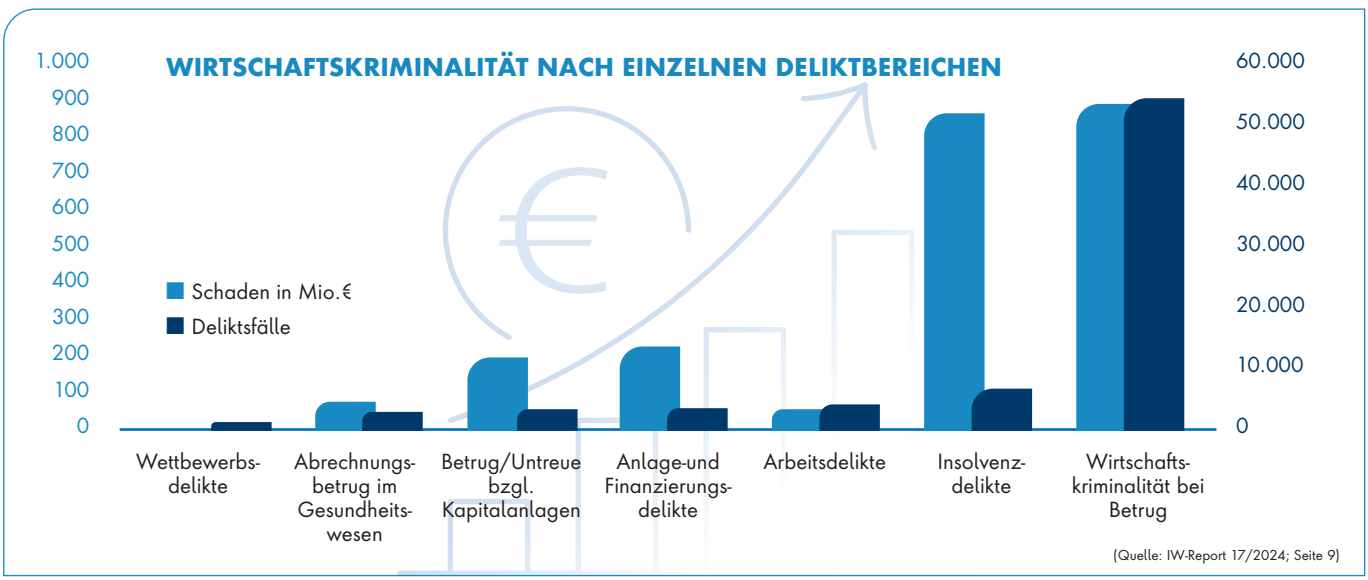
Die Zunahme von Finanzbetrug und Wirtschaftskriminalität macht vor keiner Branche halt und betrifft alle Akteure, von Finanzinstitutionen bis hin zu staatlichen Einrichtungen. Der Skandal um Wirecard, ein markantes Beispiel für Jahresabschlussbetrug, hat dem Finanzsektor das Ausmaß solcher Verbrechen vor Augen geführt. Das Unternehmen wurde zum Schauplatz massiven Betrugs, was die Notwendigkeit strengerer regulatorischer Kontrollen im Finanzsektor betonte.

Angesichts der weitreichenden finanziellen Verluste und wirtschaftlichen Auswirkungen auf Unternehmen und die Gesellschaft insgesamt, wird immer deutlicher, wie dringend sofortige und koordinierte Präventionsmaßnahmen sind. Denn sind die Schäden erst einmal entstanden, sind die Folgen für Unternehmen und Finanzinstitute in der Regel existenzbedrohend. Diese Entwicklungen erfordern einen neuen Fokus auf Prävention im Allgemeinen und eine Neubewertung der bestehenden Prüfungsverfahren sowie eine stärkere Integration fortschrittlicher Technologien, um die Betrugserkennung an das steigende Volumen wirtschaftskrimineller Vorfälle anzupassen. Welche spezifischen Strategien können Wirtschaftsprüfer und Bankangestellte anwenden, um den Herausforderungen der zunehmenden Unsicherheit bei der Aufdeckung von Finanzbetrug wirksam zu begegnen?

Drittbestätigung im Wandel

Betrug, der immer ausgeklügeltere Formen annimmt, kann traditionelle Kontrollsysteme umgehen und macht das Aufdecken raffinierter Manipulationen unsicher und komplex. In diesem Zusammenhang kommt Wirtschaftsprüfern und Bankangestellten eine wichtige Rolle als Hüter der finanziellen Integrität zu. Doch diese Aufgabe wird immer schwieriger, da Betrüger ihre Strategien ständig verfeinern.

Der Prozess von Drittbestätigungen wie Bankauskünften ist für Jahresabschlussprüfungen entscheidend und erfordert eine komplizierte Koordination gemäß den Richtlinien des IDW-Prüfungsstandards. Die Bewältigung der wachsenden



(Quelle: IW-Report 17/2024; Seite 9)

Bedrohung durch Finanzbetrug erfordert einen umfassenden Ansatz, der über traditionelle Bestätigungsmethoden hinausgeht. Workflows in der Wirtschaftsprüfung sind in vielen Teilen noch analog. Die zuständigen Personen sind in der Regel noch daran gewöhnt, Bankbestätigungen per Post einzuholen. Neben dem offensichtlichen Zeitverlust verglichen mit der digitalisierten Version dieses Prozesses, lässt dieses Verfahren aber auch zahlreiche Türen für Wirtschaftskriminelle offen: Absender und Briefumschläge können gefälscht werden, Briefe können verloren gehen und Personen können sich für jemand anderen ausgeben. Heutzutage ermöglichen digitale Lösungen eine effizientere und automatisierte Abwicklung, bei der alle Parteien zuverlässig verifiziert werden. Modernste Technologien reduzieren den Arbeitsaufwand erheblich und verbessern die Reaktionszeit, Sicherheit und Qualität der Bestätigungsprozesse.

Strategische Innovation gegen Betrug

Die zunehmende Bedrohung zwingt Wirtschaftsprüfungsgesellschaften und Banken dazu, wachsamer zu werden und proaktive Maßnahmen zu ergreifen. Um effektive Strategien zur Betrugsbekämpfung in der Finanzprüfung zu entwickeln, ist ein ganzheitlicher und integrierter Ansatz erforderlich. Dies beinhaltet nicht nur eine umfassende Analyse potenzieller Risiken, sondern auch den Einsatz fortschrittlicher Technologien wie Künstliche Intelligenz und Maschinelles Lernen zur vorzeitigen Erkennung verdächtiger Betrugsmuster. Zudem ist eine enge Zusammenarbeit zwischen verschiedenen internen Interessenvertretern, darunter Prüfungsteams, Rechtsabteilungen und Compliance-Abteilungen, unerlässlich, um eine kontinuierliche Überwachung zu gewährleisten und schnell auf Warnsignale zu reagieren. Parallel dazu ist es entscheidend, das Bewusstsein der Mitarbeiter auf allen Ebenen zu schärfen, um eine Kultur der Regelkonformität und Verantwortlichkeit zu fördern.

Indem Prüfungsgesellschaften ihre Betrugsabwehr stärken, können sie nicht nur das Risiko von Finanzbetrug minimieren, sondern auch das Vertrauen ihrer Kunden, Partner und der Gesellschaft in die Glaubwürdigkeit und Transparenz finanzieller Transaktionen festigen. Die Integration neuer Technologien, proaktive Betrugserkennung und kontinuierliche Innovation bilden die entscheidenden Grundlagen, um die Integrität von Prüfungsgesellschaften sowie Banken in einem sich ständig wandelnden Finanzumfeld zu wahren.

Kyle Gibbons

UM EFFEKTIVE STRATEGIEN ZUR BETRUGSBEKÄMPFUNG IN DER FINANZPRÜFUNG ZU ENTWICKELN, IST EIN GANZHEITLICHER UND INTEGRIERTER ANSATZ ERFORDERLICH.

Kyle Gibbons: Managing Director Europe, Thomson Reuters Confirmation, www.eu.confirmation.com/de/

Die nächste Phase der KI-Transformation

GENERATIVE KI UND MICROSOFT (365) COPILOT ERFOLGREICH SKALIEREN

Generative KI bietet für die moderne Arbeitswelt hoch innovative und effizienzsteigernde Technologien. Diese können Unternehmen heute nutzen, um ihre Prozesse, Produkte und Services zu verbessern. Nach der Einführung von Microsoft (365) Copilot im November 2023 haben viele Unternehmen in Deutschland kurzfristig Maßnahmen initiiert, um generative KI in alltäglich genutzten Tools des digitalen Arbeitsplatzes anwendbar zu machen. Somit konnten sie erste Erfahrungen mit diesen neuen Werkzeugen im kleinen Rahmen sammeln: Sei es in Workshops, Evaluations-Projekten oder Teilprozess-Optimierungen.

Doch wie geht es weiter? Wie können Unternehmen die Nutzung der vielfältigen Technologien ausweiten, vertiefen und ganzheitlich ausrollen? In der nächsten Phase brauchen Organisationen eine KI-Strategie und Transformationsplanung, um die Ziele, Erfolgskriterien und Handlungsfelder ihrer KI-Initiativen festzulegen. Eine solche KI-Strategie fehlt in vielen Unternehmen aber oder wurde noch nicht auf die neuen Möglichkeiten von generativer KI mit Microsoft (365) Copilot angepasst.

Was eine KI-Strategie und KI-Transformationsplanung beinhalten sollten

In Zeiten hoher Innovationsgeschwindigkeit können KI-Strategie und Transforma-

tionsplanung keine starren Dokumente mehr sein: Bei der erwarteten schnellen technologischen Weiterentwicklung müssen sie vielmehr dynamische und iterative Instrumente werden, die von KI-Strategen und ihren Entscheidern regelmäßig überprüft und angepasst werden. Zudem ändern sich die Anforderungen zur Nutzung von generativer KI unterschiedlicher Fachbereiche heutzutage schnell, worauf nicht zuletzt die IT regelmäßig reagieren muss. Trotz dieser Dynamik gibt es einige grundlegende Elemente, die Unternehmen in ihrer KI-Strategie und Transformationsplanung berücksichtigen. Dazu einige Praxisbeispiele:

#1 Ein Visions- und Missions-Statement sowie eine KI-Themenlandkarte werden genutzt, um langfristige Ziele und prioritäre Themen für die Nutzung von KI -Instrumenten transparent zu machen.

#2 Ein klares Verständnis für die wichtigsten Use Cases ist insbesondere für die neuen Microsoft (365) Copilot Produkte notwendig, da sie die Nutzung von generativer KI auch für „Laien" ermöglichen und gleichzeitig eine Vielzahl an Anwendungsszenarien im Arbeitsalltag unterstützen.

#3 Eine Roadmap mit Etappen und Zwischenzielen für einen Rollout von Microsoft (365) Copilot und anderen KI-Instrumenten ist notwendig, um Ressourcen und Budgets im Zeitablauf zu allokieren und gleichzeitig Abhängigkeiten zu berücksichtigen.

#4 Ein Angebot zur Weiterbildung und für den Aufbau von KI-Skills bei den Mitarbeitenden ist ein Erfolgsfaktor, um Akzeptanz und Vertrauen in die Technologien zu fördern und den bestmöglichen Nutzen zu realisieren.

#5 Ein Governance-Framework für die Zusammenarbeit zwischen IT und Business wird angewendet, um die sich ständig weiter entwickelnden Anforderungen der Fachbereiche professionell zu managen. Daneben helfen Richtlinien und Standards, um einen Wildwuchs von KI-Tools zu verhindern und Datensicherheit zu gewährleisten.

> MIT DER BEREITSTELLUNG VON GENERATIVER KI IN MICROSOFT (365) COPILOT HABEN UNTERNEHMEN NEUE, UNGEAHNTE MÖGLICHKEITEN ZUR PRODUKTIVITÄTSSTEIGERUNG IM ALLTÄGLICHEN UMFELD EINES DIGITALEN ARBEITSPLATZES MIT MICROSOFT 365 AN DIE HAND BEKOMMEN.
>
> **Sven Hausen,**
> **Associate Partner | Transformation of Work, Campana & Schott,**
> **www.campana-schott.com**

#6 KI Communities werden etabliert, um die Erfahrungen und die Best Practices der Anwender auszutauschen und zu kommunizieren.

Microsoft Copilot Extensions

Im nächsten Schritt gibt es neben der KI-Strategie einen weiteren strategischen Aspekt, den IT-Strategen für ihre Roadmap-Planung berücksichtigen sollten, wenn generative KI mit Microsoft (365) Copilot in Unternehmen skaliert wird: die Copilot Extensions. Dabei handelt es sich um Plug-Ins und Konnektoren, die es zum einen ermöglichen, individuelle Copilot Apps zu implementieren. Zum anderen kann man die KI-Welt von Microsoft mit anderen Plattformen verbinden, wie zum Beispiel mit Service Now, Salesforce. Das hat mehrere Vorteile:

#1 So können Prozesse über Systemgrenzen hinweg optimiert und mittels generativer KI automatisiert werden, beispielsweise bei der Erstellung von Texten, dem Ausfüllen von Formularen oder der Beschleunigung von Workflows.

#2 Mit maßgeschneiderten und integrierten KI-Lösungen bieten IT-Abteilungen ihren internen Kunden deutlich mehr Möglichkeiten, um deren spezifischen Anforderungen zu erfüllen.

#3 Die Flexibilität und die Skalierbarkeit von KI-Lösungen wird durch den Ansatz der Copilot Extensions insgesamt verbessert.

Fazit

Mit der Bereitstellung von generativer KI in Microsoft (365) Copilot haben Unternehmen seit kurzem neue, ungeahnte Möglichkeiten zur Produktivitätssteigerung im alltäglichen Umfeld eines digitalen Arbeitsplatzes mit Microsoft 365 an die Hand bekommen. Um die daraus resultierenden Potenziale für ein Unternehmen zu heben bedarf es weit mehr als eine simple Verprobung durch eine beschränkte Anzahl an Anwendern im ersten Schritt bieten kann. In der nächsten Phase der KI-Transformation werden Unternehmen dazu übergehen, die Möglichkeiten von generativer KI in eine neue oder erneuerte KI-Strategie und Transformationsplanung zu integrieren. Nur so können sie smart investieren und die zukünftige Wettbewerbsfähigkeit durch höhere Prozesseffizienz steigern.

Sven Hausen

Microsoft (365) Copilot

ERFAHRUNGEN AUS DER PRAXIS

Viele Unternehmen wollen von KI profitieren. Doch wo bringen Tools wie Microsoft (365) Copilot echte Vorteile und was ist bei der Einführung und Nutzung zu beachten? Marco Heid, Head of Content & Collaboration bei Campana & Schott, berichtet aus der Praxis.

it management: *Herr Heid, viele Unternehmen beschäftigen sich aktuell mit Generativer KI. Wo liegen die größten Herausforderungen?*

Marco Heid: Anfangs ist oft eine große Begeisterung der Belegschaft zu spüren, die jedoch schnell nachlässt. Wir stellen häufig fest, dass in Unternehmen, die einfach Lizenzen ausgerollt haben, ohne den Rollout zu begleiten oder die Erwartungen zu steuern, sich oft wieder die gewohnten Arbeitsweisen durchsetzen.

Um KI-Tools fest zu verankern, sollten Unternehmen auf einen Dreiklang aus Strategie, Readiness und Adoption setzen. Unternehmen müssen eine passende Strategie entwickeln, um mit KI die größten Vorteile zu erzielen. Der Datenbestand muss geprüft und aufbereitet, also KI-ready gemacht werden. Denn Generative KI ist nur so gut wie der zugrundeliegende Content. Es braucht auch eine dauerhafte Change-Begleitung.

it management: *Fachbereiche haben oft verschiedene Anforderungen. Wie können Unternehmen ermitteln, welche Use Cases am vielversprechendsten sind?*

Marco Heid: Es lohnt sich, die Standard Use Cases in Microsoft (365) Copilot zu betrachten. Dazu gehören etwa automatische Zusammenfassungen von Online-Meetings und die Erstellung von Aufgabenlisten. Anhand von empirischen Studien wie etwa den Work Trend Index von Microsoft lassen sich ebenfalls bewährte Use Cases ermitteln. Zusätzlich sollten in Workshops mit den Fachbereichen Verbesserungspotenziale in deren Arbeitsalltag identifiziert werden.

it management: *Welche konkreten Use Cases und Aufgaben werden bereits jetzt sehr gut mit KI gelöst?*

Marco Heid: Dazu gehören etwa das Vorbereiten und Optimieren von Texten und Präsentationen sowie die Erzeugung von Bildern mit Hilfe natürlicher Spracheingaben. Durch die Eingabe natürlicher Sprache und gezieltere Ergebnisse wird KI wohl auch bei der Recherche und Informationsbeschaffung langfristig die klassische Suche ersetzen. Künftig lassen sich komplexere Aufgaben wie eine vollständige Reiseplanung in einem Schritt und mit Rückfrageschleifen durchführen.

it management: *Welche Stärken und Schwächen weist Copilot im Vergleich zu anderen KI-Tools wie ChatGPT auf?*

Marco Heid: Die große Stärke von Microsoft (365) Copilot ist die Integration in die Microsoft Office-Welt, KI-Funktionen können direkt in Teams, Word oder Outlook genutzt werden. Zusätzlich kann der Microsoft (365) Copilot geschäftliche Dokumente und Informationen in Antworten mit einbeziehen und somit spezifisches Unternehmenswissen verarbeiten. Das bedeutet einen geringen Implementierungsaufwand für das Unternehmen, viele Drittsysteme wie Salesforce oder SAP lassen sich direkt anbinden. Zudem bietet Copilot im Vergleich zu kostenlosen Tools ein deutlich höheres Niveau an Sicherheit und Datenschutz.

it management: *Wie sieht ein typisches Projekt zur Einführung von Copilot aus?*

COPILOT BIETET IM VERGLEICH ZU KOSTENLOSEN TOOLS EIN DEUTLICH HÖHERES NIVEAU AN SICHERHEIT UND DATENSCHUTZ.

Marco Heid,
Head of Content & Collaboration,
Campana & Schott,
www.campana-schott.com

Marco Heid: Wir begleiten Unternehmen meist über Monate durch das gesamte Projekt, von der Planung und Pilotierung über die Durchführung bis zur Rollout-Begleitung. Dies beginnt häufig mit dem Schärfen der KI-Strategie sowie der Identifizierung der Use Cases. Wir erstellen Leitfäden und Prompts für die Personas, entwickeln Extensions, setzen Communities auf und strukturieren das Projekt. Wir sorgen auch für die Readiness, unterstützen das Change & Adoption Management und führen mit Hilfe eines von uns entwickelten Kalkulators eine Business-Value-Analyse durch. So erhalten Unternehmen eine umfassende Unterstützung aus einer Hand und auf Augenhöhe.

it management *Herr Heid, wir danken für das Gespräch.*

THANK YOU

Optimierte Geschäftsabläufe dank KI

KÜNSTLICHE INTELLIGENZ BRINGT PROZESSMANAGEMENT AUF EINE NEUE EBENE

Künstliche Intelligenz ist bei der digitalen Transformation von Branchen und Geschäftsfeldern nicht mehr wegzudenken. Insbesondere im Bereich des Business Process Managements (BPM), also der Steuerung und Optimierung von Geschäftsprozessen, bietet der Einsatz von KI-Technologien enorme Vorteile. Mit ihrer Hilfe können datenbasierte Muster und Trends erkannt und zur Erstellung von optimierten Prozessstrukturen genutzt werden.

Für Unternehmen bietet KI enorme Vorteile, zum Beispiel in der Kundenbetreuung oder auch in Bezug auf die eigene Entwicklung. So können Routinetätigkeiten automatisiert werden, wodurch wiederum Mitarbeiterressourcen für andere Tätigkeiten, wie strategische Aufgaben, frei werden. Darüber hinaus bietet die KI-gestützte Optimierung und Automatisierung von Geschäftsprozessen Verbesserungspotenziale für Unternehmen von Effizienzsteigerung über Risikominderung und Fehlervermeidung bis hin zur Förderung von Innovationen.

Entwicklungen im KI-gestützten BPM

Ein Unternehmen, das sich bereits intensiv mit dem Thema KI beschäftigt, ist Inspire Technologies. Unter dem Namen MR. KNOW bietet es eine Software an, mit der Unternehmen und Behörden ihre Geschäftsprozesse digital erfassen, optimieren und automatisieren können. Geschäftsführer Dr. Michael Otte und sein Team forschen aktuell zu möglichen Anwendungsgebieten für die Verwendung von KI und haben nun eine erste Integration in der MR.KNOW-Plattform vorgestellt: „Wie bringt künstliche Intelligenz unseren Kunden den größten Nutzen? Ganz einfach: KI ermöglicht es einerseits, MR.KNOW interaktiver für Prozesse und digitale Assistenzen zu gestalten. Andererseits haben wir KI in die Prozesserstellung integriert. Somit kann jeder das weltweite Wissen von KI nutzen und sich Vorschläge für Prozesse und Lösungen erstellen lassen."

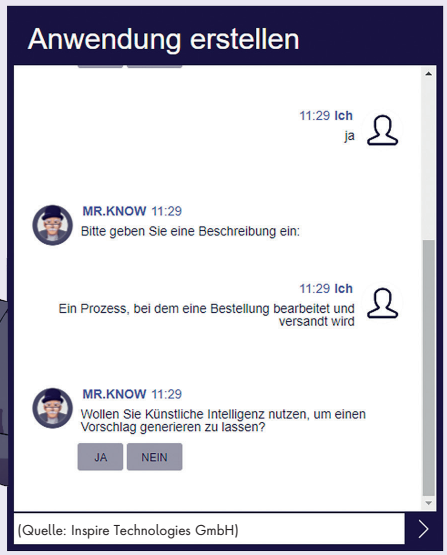
KI-basierte Prozessmodellierung

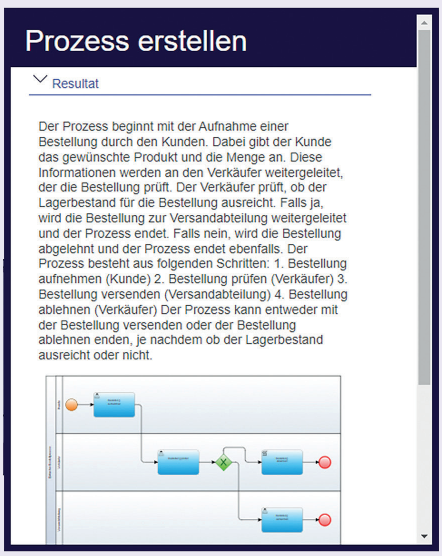
Die Kombination von künstlicher Intelligenz und No Code-BPM, also Business Process Management ohne Programmierung, bietet Unternehmen die Möglichkeit, auch ohne Programmierkenntnisse oder Fachkenntnisse im Bereich der Prozessmodellierung eigenständig digitale Assistenten und komplette Lösungen zu erstellen. Dabei generiert die KI im ersten Schritt aus einer Idee einen konkreten Lösungsvorschlag. Die Software wandelt den entsprechenden KI-Code wiederum in ein Prozessmodell im Standard BPMN 2.0 um. Das so entstandene Prozessmodell kann im nächsten Schritt über eine grafische Nutzeroberfläche an die eigenen Anforderungen angepasst und als eigene Lösung sicher gespeichert werden. Der Nutzer selbst kann so auf das Wissen von Millionen Anwendern zurückgreifen, um seine eigene, individuelle Lösung zu erhalten. Somit können Anwender ohne Vorwissen einfach und schnell starten, aber auch komplexe Prozessanwendungen umsetzen. Darüber hinaus können die KI-gestützten Modelle kontinuierlich angepasst werden, um Prozesse weiter zu verbessern und auf Veränderungen im Geschäftsumfeld zu reagieren.

Die Integration von künstlicher Intelligenz in das Business Process Management verspricht Unternehmen also nicht nur Unterstützung bei der Optimierung ihrer Prozesse, sondern setzt auch neue Maßstäbe in Sachen Flexibilität, Reaktionsfähigkeit und Wettbewerbsfähigkeit.

Andreas Mucke | www.mrknow.ai

Künstliche Intelligenz für Prozessvorschläge nutzen





AI Act: Fortschritt oder Bremse?

WARUM BRAUCHT ES NEBEN DER DSGVO WEITERE REGULIERUNGEN FÜR KI?

Spätestens im Jahr 2025 soll der AI Act in Kraft treten, der nicht nur die Funktionsweise von Tech-Giganten und KI-Startups in Europa verändern, sondern auch Auswirkungen auf die Cybersicherheit von Unternehmen haben wird. Davon sind besonders Unternehmen betroffen, die kritische Infrastrukturen betreiben oder in anderen Hochrisikobereichen aktiv sind. Während die KI-Gesetzgebung ein wichtiger Schritt für die Nutzung von KI ist, unterschätzen Unternehmen oft das Ausmaß der anstehenden Gesetzgebungsverfahren. Der AI Act wurde entwickelt, um auf die Herausforderungen, die KI-getriebene Lösungen und Services hervorrufen zu regulieren, doch es weist noch Lücken auf.

Beschränkungen der DSGVO in Bezug auf KI

Die DSGVO bildet einen wichtigen rechtlichen Rahmen für den Umgang mit personenbezogenen Daten, der auch für KI-bezogene Praktiken gilt. Dabei stößt die DSGVO oft an ihre Grenzen, insbesondere wenn es um KI geht, die auf nicht personenbezogene Daten trainiert wird. Da sie in solchen Fällen nicht greift und zusätzliche Regelungen erforderlich sind. Sie schützt speziell sensible Daten gemäß Artikel 9 der Verordnung. Allerdings basiert die Erlaubnis zur Datenverarbeitung nicht allein auf der Art der Daten oder ihrer Verarbeitung. Die DSGVO berücksichtigt eine Vielzahl von Interessen, um festzustellen, ob eine Verarbeitung zulässig ist. KI, wie sie heute genutzt wird ist der DSGVO fremd. Was sich daran bemerkbar macht, dass sie potenzielle Vorteile von KI-Anwendungen für die Gesellschaft, aber auch negative Auswirkungen von KI, nicht ausreichend berücksichtigt.

Ein Beispiel dafür ist unzulässiges Profiling und unbemerkte Verarbeitung sensibler Informationen. Oft sind KI-Systeme für User eine Blackbox. Daten werden eingegeben und die KI generiert Antworten und Ergebnisse, ohne die Gewährleistung, dass geteilte Daten geschützt sind und für weitere KI-Trainingszwecke genutzt werden. Obwohl unter der DSGVO persönliche Daten vor einem Missbrauch geschützt sind, könnten KI-Systeme beispielsweise sensible Informationen extrahieren und so verwenden, dass ein Datenmissbrauch nicht sofort erkennbar ist. Was es schwieriger macht, Verstöße zu erkennen und zu bekämpfen.

DER EUROPÄISCHE AI ACT WURDE PRIMÄR KONZIPIERT, UM EINE RECHTLICHE GRUNDLAGE FÜR DEN EINSATZ UND DIE WEITERENTWICKLUNG VON KÜNSTLICHER INTELLIGENZ ZU SCHAFFEN.

Moritz Plassnig, Datensicherheits-Expterte und Chief Product Officer, Immuta, www.immuta.com

Der Einfluss von KI auf die DSGVO

Die DSGVO wird zu Zeiten von KI relevanter denn je. Ein aktuelles Beispiel dafür ist die OpenAI-Saga, die durch die italienische Datenschutzaufsicht ausgelöst wurde. Diese entschied Anfang 2024, dass ChatGPT gegen die Bestimmungen der DSGVO der EU verstößt. ChatGPT wurde daraufhin 30 Tage eingeräumt, um Gegenansprüche bezüglich der behaupteten Verstöße geltend zu machen. Im Fokus der Debatte stand der Artikel 22 der DSGVO, der ein Verbot der automatisierten Entscheidung im Einzelfall festlegt. Hier wird die Art und Weise, wie der Artikel 22 und der Schutz automatisierter Entscheidungen ausgelegt werden, einen klaren Unterschied machen und sind eines der wichtigsten Bestimmungen, die es in Zukunft zu beobachten gilt.

Nach Artikel 22 der DSGVO haben Betroffene grundsätzlich das Recht, nicht einer ausschließlich automatisierten Entscheidung unterworfen zu werden. Hierbei handelt es sich um die Entscheidung, die ohne menschliches Zutun erfolgt und nicht um die Bewertung der persönlichen Aspekte einer betroffenen Person. Dieses Recht entfällt, wenn die automatisierte Entscheidungsfindung im Rahmen von Vertragsverhältnissen erforderlich ist, die betroffene Person darüber informiert wurde und eingewilligt hat oder eben die Maßnahmen zum Schutz der Betroffenen erfolgten.

Durch Profiling und die automatisierte Entscheidungsfindung haben Unternehmen beispielsweise die Möglichkeit, Angebote und Dienstleistungen zu personalisieren, was die Kundenbindung stärken und zu Umsatzsteigerungen beitragen kann. Gleichzeitig können Unternehmen Betrugsmuster erkennen und dadurch auch schneller verhindern.

Bei einem Verstoß gegen die Vorgaben der automatisierten Entscheidungsfindung droht Unternehmen ein hohes Bußgeldrisiko. Schwerer wiegt bei einem Verstoß, dass zukünftige sowie bereits ergangene Verarbeitungstätigkeiten eingestellt und rückgängig gemacht werden müssen. Missachten Unternehmen den Artikel 22 kann das schwere finanzielle Folgen nach sich ziehen.

Zeitfaktor bei der Umsetzung von KI-Regulierungen

Die Diskussion und Festlegung von KI-Regulierungen werden durch verschiedene politische und wirtschaftliche Interessen beeinflusst, was oft zu Verzögerungen in der Gesetzgebung führt. Auf der einen Seite gibt es Befürworter eines „Pro-Wachstums"-Ansatzes, die Innovationen fördern möchten. Auf der anderen Seite stehen diejenigen, die einen ausgewogenen Ansatz befürworten und dabei die potenziellen systemischen Risiken im Zusammenhang mit der Bereitstellung von KI-as-a-Service oder der Freigabe von Open-Source-Modellen berücksichtigen. Jede gesetzliche Regelung ist ein politischer Kompromiss, der viel Zeit und Geduld erfordert.

Die Herausforderungen des europäischen AI Acts

Der europäische AI Act wurde primär konzipiert, um eine rechtliche Grundlage für den Einsatz und die Weiterentwicklung von Künstlicher Intelligenz zu schaffen. Allerdings gibt es diverse Faktoren, die bei der KI-Gesetzgebung zu berücksichtigen sind. Zwar ist es wichtig, spezifische Situationen und Anwendungsfälle einzubeziehen, jedoch birgt dies das Risiko, dass das Gesetz dadurch nicht streng genug ausgelegt wird. Besonders durch zahlreiche Ausnahmen könnte das Gesetz geschwächt werden, was letztlich seine Wirksamkeit mindern könnte.

Ein weiteres Problem liegt darin, dass der AI Act keinen klaren Rahmen vorgibt, um zu prüfen, ob KI-Systeme den Richtlinien entsprechen. In dieser Hinsicht sind Organisationen auf sich allein gestellt und müssen eigene Prozesse und Standards entwickeln, um ihre KI-Systeme sorgfältig zu überwachen. Somit hängt der Erfolg des AI Acts stark von der Arbeit dieser Prüfstellen und der Qualität der Aufsichtsbehörden ab. In Bezug auf den Datenschutz sollten Standards und Prüfungen den Fokus auf Prozesse legen und nicht ausschließlich auf die Inhalte der KI-Systeme. Letztlich ist die Effektivität des KI-Gesetzes stark von der konsequenten Durchsetzung abhängig. Es ist zu erwarten, dass die Akzeptanz von KI in verschiedenen Bereichen unterschiedlich schnell erfolgen wird. Insbesondere in Bereichen wie Justiz, Bildung und Sozialleistungen sollten KI-Anwendungen besonders sorgfältig überwacht werden, da dort die Auswirkungen oft gravierend sein können.

Verantwortung und Evaluation in der KI-Entwicklung

Obwohl der AI Act einen vielversprechenden Schritt für die KI-Entwicklung in Europa darstellt, bestehen weiterhin einige Herausforderungen, die angegangen werden müssen, um ein solides Regelwerk zu etablieren. Es ist außerdem entscheidend, dass der Faktor Mensch weiterhin im Mittelpunkt steht. Unternehmen sollten daher die Eigenverantwortung übernehmen und ihre KI-Systeme sowie die dazugehörigen Prozesse sorgfältig evaluieren. Ziel ist es sicherzustellen, dass ihre Lösungen und Dienste, Menschen unterstützen und nicht gefährden.

Moritz Plassnig

Vierfach fit für die E-Rechnung

TOOLS FÜR MICROSOFT DYNAMICS 365 BUSINESS CENTRAL NUTZEN

Die E-Rechnung in deutschen Unternehmen – ein Selbstläufer? Ein Blick in eine Studie des Branchenverbands bitkom aus dem vorigen Jahr stimmt zunächst optimistisch: Haben 2016 noch 58 Prozent der befragten Unternehmen auf papierbasierte Rechnungen gesetzt, waren es 2022 nur noch ein Viertel, Tendenz weiter sinkend. 40 Prozent gaben an, überwiegend elektronische Rechnungen zu schreiben. Doch im Detail zeigen sich deutliche Unterschiede bei großen, mittelgroßen und kleinen Betrieben.

Während 9 von 10 Unternehmen mit mehr als 500 Mitarbeitenden die gängigen E-Rechnungsformate (wie ZUGFeRD und XRechnung) bereits einsetzen, konnte dies nicht einmal jedes zweite Unternehmen bis 99 Mitarbeitende von sich behaupten. Innerhalb des letzten Jahres dürfte sich zwar noch einiges bewegt haben. Dennoch hat der Mittelstand noch Nachholbedarf bei der E-Rechnung – und die Pflicht rückt unaufhaltsam näher. Die gute Nachricht: Manchmal braucht es weniger als gedacht, um fit für die E-Rechnung zu werden.

Das kleine Einmaleins der E-Rechnungs-Fitness

Was aber vielen nicht klar ist: Es reicht nicht aus, E-Rechnungen ab 2025 empfangen und später auch versenden zu können. „E-Rechnungs-Fitness hat vier Disziplinen", erklärt Mario Koch vom Technologie- und Managed Service Provider Konica Minolta: „Neben der Verarbeitung von Eingangsrechnungen gehört auch die Compliance-konforme digitale Ablage dieser Rechnungen dazu. Denn die GoBD schreibt vor, dass ich kaufmännische Belege in derselben Form archiviere, wie ich sie empfange." Gleiches gilt für ausgehende Rechnungen. „Wenn ich E-Rechnungen versende, kann ich sie nicht in Papierform ausdrucken und abheften. Ich muss sie auch unverändert nach dem Versand digital vorhalten."

E-Rechnungen und Archiv sind oft keine Standard-Funktion

Um diese vier Disziplinen mit Bravour zu beherrschen, müssen die wenigsten Unternehmen bei null anfangen – doch kleine Details fehlen oft. Das zeigt sich am Beispiel Microsoft Dynamics 365 Business Central. „Business Central ist ein ERP-System und kaufmännische Applikation, welche die Unternehmensprozesse sehr gut abbildet. Mit dem Verwalten von Belegen hat sie erstmal wenig zu tun", erklärt Software-Experte Mario Koch. Deshalb fehle das Erstellen, Verarbeiten und GoBD-konforme Archivieren von Eingangs- und Ausgangsrechnungen im Standard-Funktionsumfang. Seine Empfehlung: „Statt Rechnungen händisch zu konvertieren und ins System zu zwängen, kann man Dynamics

365 Business Central mit wenig Aufwand erweitern – und dabei viel mehr erreichen als nur die Pflicht zu erfüllen." Hierfür schlägt er konkrete Tools vor.

TOOL-TIPP 1 E-Rechnungen versenden: forNAV

Das Spezialgebiet von forNAV sind Dynamics-Erweiterungen für komfortable Reporting- und Exportfunktionen. Der Name täuscht, denn der Anbieter entwickelt heute kaum noch Lösungen für die Vorgängerversion Microsoft Dynamics NAV, sondern schwerpunktmäßig für 365 BC. Die forNAV-Lösung zur Erstellung von E-Rechnungen unterstützt neben dem führenden ZUGFeRD-Standard auch XRechnung und Factur-X. „Das Tool funktioniert denkbar einfach", erläutert Mario Koch: „Erweiterung mit wenigen Klicks installieren – und sofort E-Rechnungen aus gängigen Reports oder Word-Dokumenten erzeugen."

TOOL-TIPP 2 E-Rechnungen empfangen: CONTINIA

Ein großer Teil der E-Rechnungen wird zukünftig im ZUGFeRD-Format eingehen – und damit auch eine für Menschen lesbare PDF-Datei enthalten. „Die Versuchung ist groß, die Rechnungen also wie bisher einfach auszudrucken, abzutippen und abzuheften. Das ist aber nicht im Sinne des Gesetzes", gibt Mario Koch zu bedenken. „Mit einem guten Tool, wie CONTINIA Document Capture, wird neben der Rechnung auch die Verarbeitung digital. Die Erweiterung kann E-Rechnungen empfangen und zum Beispiel die Prüfung innerhalb von Business Central direkt abbilden." Auf diese Weise ist die E-Rechnung der erste Schritt, um ganze Prozesse zu automatisieren – also effizienter, schneller und weniger fehleranfällig zu arbeiten.

TOOL-TIPP 3 E-Rechnungen archivieren: ECM smart connect

Um E-Rechnungen nicht nur rechtssicher zu archivieren, sondern auch leicht auffindbar und nutzbar zu machen, empfiehlt Mario Koch „ECM smart connect" als Schnittstelle zwischen Dynamics 365 BC und einem vorhandenen ECM-System. „Das Tool integriert sich nahtlos in die Business Central Oberfläche. Alle Belege, Aufträge, Lieferscheine und Rechnungen, die ich dort erhalte oder erzeuge, werden dann samt Metainformationen in einer digitalen Lieferanten- oder Kundenakte abgebildet. Per Drag-and-Drop kann man beliebige Dokumente aus verschiedenen Quellen hinzufügen." ECM smart connect unterstützt d.velop, ELO, Shareflex M365 und demnächst auch EASY.

TOOL-TIPP 4 Ausgangsrechnungen samt Belegen archivieren: ELO, d.velop & Co.

Wer ein vorhandenes ECM-System mit Microsoft Dynamic 365 BC verknüpft oder eines implementiert, kann Eingangs- genauso wie Ausgangsrechnungen über Kontext- oder Volltextsuche auffindbar machen – und GoDB- sowie DSGVO-konform archivieren, inklusive Löschfristen. „Es ist aber noch mehr möglich", verdeutlicht ECM-Experte Mario Koch: „Ich kann sämtliche Daten, Dokumente und Belege, die für die Rechnung relevant sind, damit in Verbindung setzen. Und zwar nicht als zehnte Kopie derselben PDF-Datei, sondern als Verknüpfung zu einer eindeutigen und versionierten Datei, auf die nur berechtigte Personen Zugriff haben und bei der Änderungen protokolliert werden. Und sogar das ist erst der Anfang."

Digitale Prozesse durchstarten

Mit der Fitness in allen vier Disziplinen ist die nächste Stufe der digitalen Transformation nicht weit: digitale und automatisierte Prozesse. Durch die Kombination von Microsoft Dynamics 365 BC und einem ECM-System ergeben sich laut Mario Koch viele Synergie-Effekte. „Vielleicht sind es Dokumentenprozesse, die langsam sind. Oder das Vertragsmanagement. Manchmal lohnt es sich auch, die Personalakte zu digitalisieren. All das ist mit den Tools möglich, die sich im Zuge der E-Rechnungspflicht ohnehin anbieten. Der Appetit kommt beim Essen."

ES REICHT NICHT AUS, E-RECHNUNGEN AB 2025 EMPFANGEN UND SPÄTER AUCH VERSENDEN ZU KÖNNEN.

Mario Koch, Head of ECM, Konica Minolta Business Deutschland GmbH, www.konicaminolta.de

Worauf noch warten?

Doch zunächst steht die E-Rechnungspflicht im Fokus. Mario Koch rät dazu, zeitnah die eigene Fitness in den vier Disziplinen zu checken. „Wenn ich überall ein Häkchen setzen kann, ist alles gut. Wenn ich ein Häkchen offen habe, dann muss ich dort zügig nachbessern." Dabei unterstützen sein Team und er gerne – als versierter Microsoft-Partner mit über 20-jähriger Erfahrung mit ECM-Lösungen und über 800 Referenzkunden in diesem Bereich. Durch den Fokus auf transparente Beratung und eine Multi-Vendor-Strategie biete Konica Minolta individuell abgestimmte Lösungen an, die optimal zum Unternehmen passen, so Koch. Und bis diese im Einsatz sind, muss es gar nicht lange dauern: „Innerhalb von zwei bis drei Monaten haben wir die E-Rechnungs-Tools für Dynamics 365 BC-User implementiert."

www.konicaminolta.de

MEHR WERT
Die eRechnung kommt

Bremsklötze der IT-Transformation

DATENQUALITÄT UND FACHKRÄFTEMANGEL SIND DIE GRÖSSTEN HÜRDEN

Bereits zum dritten Mal in Folge haben Natuvion und die NTT DATA Business Solutions Top-Manager und Abteilungsleiter danach befragt, wie sie die Transformation ihrer IT-Landschaft in den zurückliegenden zwei Jahren bewältigt haben. Die Ergebnisse der internationalen, in 15 Ländern durchgeführten Studie zeigen, dass Unternehmen die Modernisierung ihrer IT-Systeme nach wie vor oft unterschätzen.

Doch es gibt durchaus auch Erfreuliches zu vermelden, denn über alle Regionen hinweg haben immerhin 57 Prozent aller befragten Unternehmen gesagt, dass sie die sich selbst gesteckten Ziele erreicht haben; 43 Prozent konnten diese hingegen nicht vollständig realisieren. Alleiniger Spitzenreiter sind die NORDICS-Staaten. Sie gaben zu 62,5 Prozent an, ihre Ziele erreicht zu haben. Die Ergebnisse der DACH-Region dagegen liegen leicht unter dem Durchschnitt der internationalen Zahlen. In Deutschland, Österreich und der Schweiz konnten 55 Prozent ihre Ziele nicht erreichen und 45 Prozent blieben hinter ihren Erwartungen zurück.

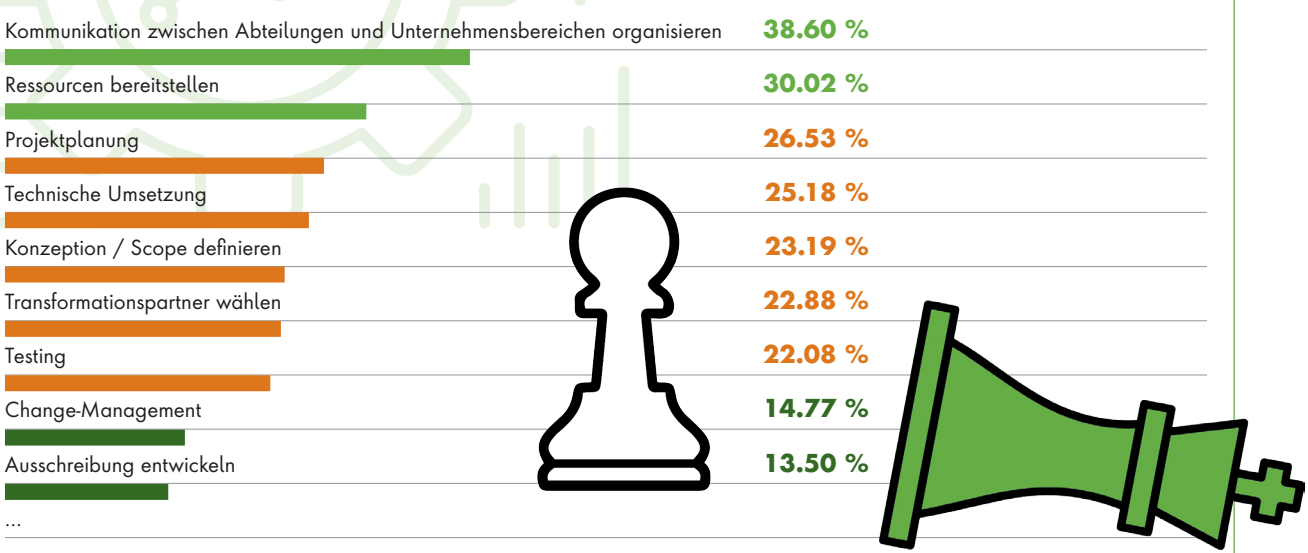
ALS ZUSÄTZLICHER BREMSKLOTZ AUF DEM WEG ZU EINER NEUEN, LEISTUNGSFÄHIGEN IT ERWEIST SICH DAS FEHLENDE TRANSFORMATIONS-KNOW-HOW.

Philipp von der Brüggen, CMO, Natuvion, www.natuvion.com

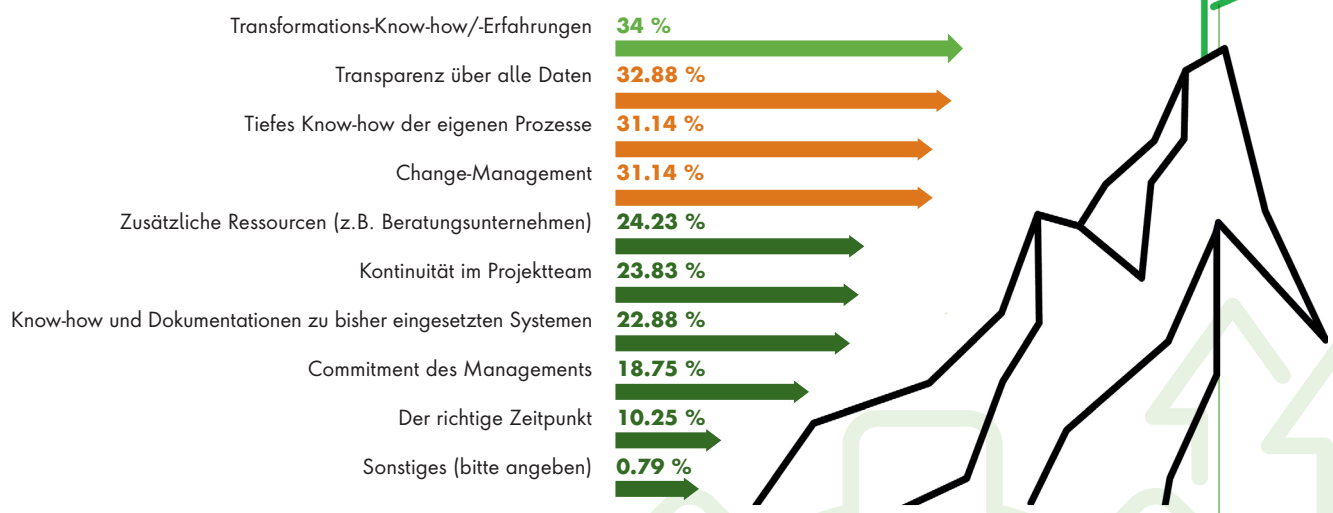
Transformationshürden

Als einer der häufigsten Stolpersteine auf dem Weg zu einem modernen IT-System entpuppte sich die Datenqualität. Auf die Frage, welche technische Maßnahme bei der Transformation von entscheidender Bedeutung war, nannten knapp 45 Prozent die Steigerung der Datenqualität.

WELCHEN TEIL IHRES TRANSFORMATIONSPROJEKTES HABEN SIE AM MEISTEN UNTERSCHÄTZT?



WAS WAREN DIE WICHTIGSTEN ERFOLGSFAKTOREN IM TRANSFORMATIONSPROZESS?



In Deutschland lag dieser Wert mit 55 Prozent sogar noch um 10 Prozent höher. Auffällig ist zudem, dass im Finanzsektor und der IT-Industrie dieser Wert ebenfalls deutlich über 50 Prozent lag. Dass bei der Frage nach der wichtigsten technischen Maßnahme die „Bestandserfassung" mit über 34 Prozent auf Platz 3 zu finden war, erscheint vor diesem Hintergrund nur logisch. Mit 42 Prozent lag Deutschland deutlich über dem internationalen Schnitt. In diesen Kontext passt, dass deutsche Unternehmen bei der Frage, welche Herausforderungen und Schwierigkeiten im Laufe ihrer Transformation eine Überraschung gewesen seien, die schlechte Datenqualität mit ca. 30 Prozent weit vorne, auf dem dritten Platz liegt.

Als zusätzlicher Bremsklotz auf dem Weg zu einer neuen, leistungsfähigen IT erweist sich das fehlende Transformations-Know-how. Als wichtigster Erfolgsfaktor, aber auch als elementare Herausforderung bei der Planung der Transformation, wurde über alle Länder hinweg fast durchgängig das Transformations-Know-how an erste Stelle gewählt. Überrascht hat die Verantwortlichen die fehlende Erfahrung ihrer Teams beim Management derartiger Projekte (34 Prozent). Dem Aufbau neuer Kompetenzen messen infolgedessen 46 Prozent der befragten Unternehmen entscheidende Bedeutung bei. Produzierende Industrieunternehmen (56 Prozent) oder die Finanzindustrie (52 Prozent) sehen hier einen besonders großen Handlungsbedarf.

AUCH WENN DIE DIGITALE TRANSFORMATION GRUNDSÄTZLICH NICHT NEU IST, SO SIND DIE DAMIT VERBUNDENEN RAHMENBEDINGUNGEN UND HERAUSFORDERUNGEN SOWIE DEREN WIRKUNG AUFEINANDER IN JEDEM UNTERNEHMEN UNTERSCHIEDLICH.

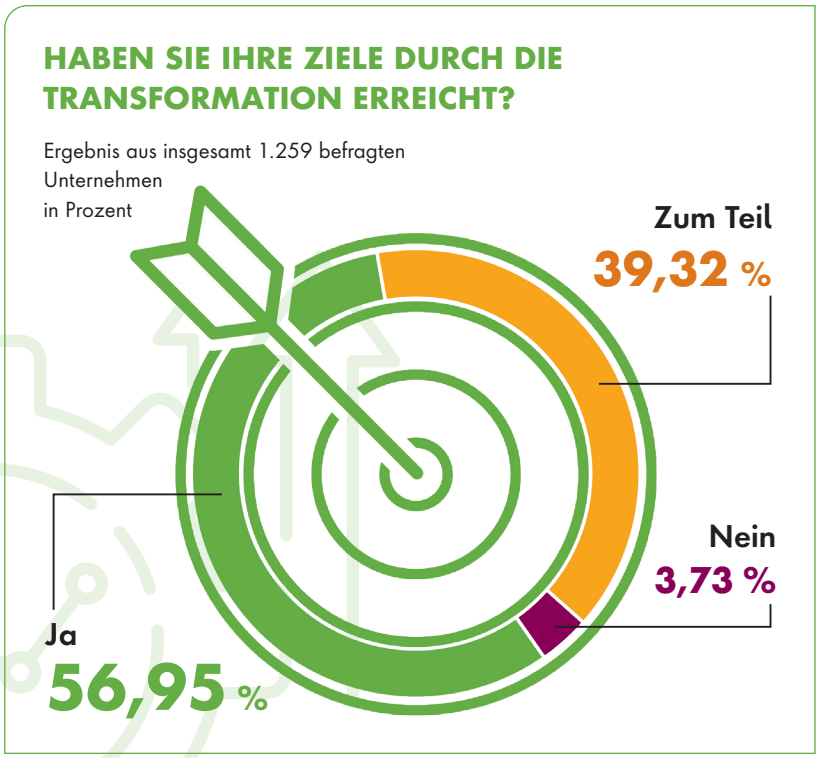
Florian Sackmann, Geschäftsleitung Customer Engagement, NTT DATA Business Solutions AG, https://nttdata-solutions.com/de/

Unterschätzt: Kommunikation und Aufwand

Dass die Renovierung der Datenverarbeitung ein reines IT-Projekt ist, ist offensichtlich falsch. Diesen Schluss jedenfalls legen die Antworten auf die Frage nahe, welcher Teil des Transformationsprojektes am meisten unterschätzt wurde: Ca. 39 Prozent der Befragten haben demnach die „Organisation der Kommunikation zwischen Abteilungen und Unternehmensbereichen" verkannt, denn diese Antwortmöglichkeit landete mit weitem Abstand auf Platz 1. Hier wird deutlich, dass eine enge Zusammenarbeit und Abstimmung zwischen der IT und den Fachbereichen keine übliche Praxis ist. Hinzu kommt, dass durch flexible Arbeitsmodelle u.a. die Arbeit aus dem Homeoffice zunimmt, was die Kommunikation darüber hinaus erschwert. In Branchen wie Life Science (42,4 Prozent), Automotive (42,4 Prozent) oder IT (44 Prozent) gaben sogar über 40 Prozent der befragten Unternehmen an, die Relevanz der Kommunikation zwischen Abteilungen und

Unternehmensbereichen falsch eingeschätzt zu haben.

Auch bei der Zeit- oder Budgetplanung stimmen Einschätzung und Realität nur selten überein. Danach befragt, was die Unternehmen aus heutiger Sicht im Rahmen der Transformation anders machen würden, belegen die drei vorderen Ränge „mehr Zeit einplanen" (ca. 37 Prozent), „mehr Ressourcen einplanen" (36,5 Prozent) und „sich früher mit der Thematik befassen" (ca. 34 Prozent). Die produzierende Industrie würde sogar zu 49 Prozent mehr Zeit einplanen. Bei den befragten Vorständen geben 44 Prozent an, dass sie sich bei einer erneuten Transformation viel früher mit dem Thema befassen würden. Diese Antworten zeigen, dass es eine durchaus signifikante Differenz zwischen der Erwartungshaltung gegenüber der digitalen Transformation und ihrer faktischen Umsetzung gibt - nicht zuletzt seitens der Unternehmensführung.



Erwartungshaltung

Der weit überwiegende Teil, 56 Prozent, der international befragten Unternehmen setzt nach der Transformation mehr Cloud-Dienste ein als davor. Von der Nutzung der Cloudservices versprechen sich 39 Prozent eine höhere Flexibilität. 38 Prozent erhoffen sich eine Beschleunigung von Geschäftsprozessen und 37 Prozent einen schnelleren und leichteren Zugang zu technischen Innovationen. Interessant: Kostenvorteile erwarten sich nur wenige vom Wechsel in die Cloud – lediglich 11 Prozent.

Zum ersten Mal beschäftigte sich die Studie von Natuvion und NTT DATA Business Solutions mit dem Thema KI. Gefragt wurde nach der Rolle von KI im Rahmen der Transformation. Etwa ein Viertel aller Unternehmen verriet, dass KI ein entscheidender Treiber für die digitale Transformation gewesen sei. Auch wenn diese Zahl auf den ersten Blick überzeugend wirkt, so relativiert sie sich doch im Vergleich zur treibenden Funktion des Datenschutzes. Auf die Frage welche Rolle der Datenschutz beim Transformationsprojekt gespielt hat, bezeichneten 34 Prozent dieses Thema als relevanten Treiber – das sind 10 Prozent mehr als bei KI. Für 21 Prozent hatte KI im Rahmen ihres Transformationsprojektes keinerlei Relevanz – beim Datenschutz waren das lediglich 9,6 Prozent.

Fazit

Auch wenn die digitale Transformation grundsätzlich nicht neu ist, so sind die damit verbundenen Rahmenbedingungen und Herausforderungen sowie deren Wirkung aufeinander in jedem Unternehmen unterschiedlich. Dennoch hat die Transformationsstudie herausgefunden, dass – anders als vielfach erwartet - KI bisher eine untergeordnete Rolle spielt, der Mangel an kompetenten Mitarbeitern aber ein weitaus folgenschwereres Problem ist als weithin angenommen. Darüber hinaus ist verwunderlich, dass die zahlreichen Aufklärungskampagnen über die erfolgreiche Umsetzung von Transformationsprojekten kaum greifen und der Zeit-, Ressourcen- und Kostenaufwand nach wie vor unterschätzt wird. Die Aufgabe der Transformationsexperten und IT-Verantwortlichen ist es deshalb, nicht müde zu werden, und auch zukünftig intensiv über die Herausforderungen und Best Practices bei der Transformation zu sprechen. Die Studie und ihre Ergebnisse tragen dazu einen wichtigen Beitrag bei.

Philipp von der Brüggen
Florian Sackmann

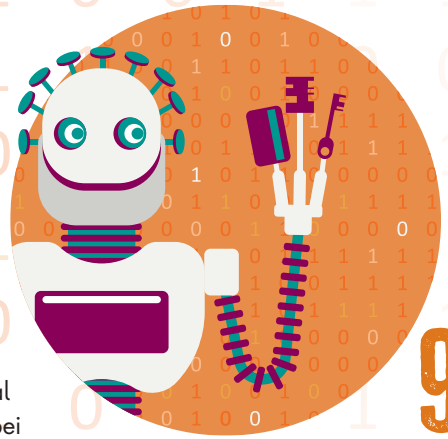
PLUS

Transformationsstudie 2024

Die vollständige Studie steht als Download zur Verfügung

Finanzkriminalität

DIGITALER BETRUG DURCH KÜNSTLICHE INTELLIGENZ



40 %

der Befragten bemängeln, dass ihr Unternehmen Betrug und Finanzkriminalität in getrennten Abteilungen behandeln

90 %

sind der Meinung, Finanzinstitute und Behörden müssen mehr Informationen austauschen, um Betrug zu bekämpfen

BioCatch hat seinen jährlichen Bericht über Betrug und Finanzkriminalität mit Schwerpunkt auf künstlicher Intelligenz (KI) veröffentlicht. Der Bericht zeigt eine beunruhigende Entwicklung: Cyberkriminelle nutzen KI und können bessere, umfassendere und erfolgreichere Betrugsversuche auf Banken und die Finanzbranche durchführen. Dafür benötigen sie kaum Bankexpertise oder technisches Know-how. Fast 70 Prozent geben an, dass die Angreifer KI geschickter einsetzen als Banken ihrerseits bei der Bekämpfung der Attacken. Ebenso besorgniserregend ist, dass etwa die Hälfte der Befragten mehr Angriffe im letzten Jahr festgestellt haben oder für 2024 erwarten.

„Künstliche Intelligenz optimiert jeden erdenklichen Betrug", sagt Tom Peacock, Director of Global Fraud Intelligence bei BioCatch. „Sie lokalisiert Sprache und Eigennamen perfekt, sodass für jedes Opfer personalisierte Betrugsversuche entstehen – mit Bildern, Videos oder Audio-Inhalten. Damit ermöglicht KI grenzenlose Betrügereien. Und das erfordert neue Strategien und Technologien der Finanzinstitute, um Kunden zu schützen."

MEHR WERT
2024 AI, Fraud, and Financial Crime Survey

Betrugsfälle durch synthetische Identitäten

Überraschend war besonders ein Ergebnis: 91 Prozent der Befragten geben an, dass ihr Unternehmen bei wichtigen Kunden die Sprachverifizierung überdenkt. Der Grund hierfür ist die Stimmerzeugung durch KI. Bei 70 Prozent haben Finanzinstitute im letzten Jahr die Verwendung synthetischer Identitäten bei der Neukundenakquise identifiziert. Die Federal Reserve schätzt, dass bisher eingesetzte Betrugsmodelle bis zu 95 Prozent der synthetischen Identitäten nicht erkennen, die für die Beantragung neuer Konten verwendet werden. Demnach wächst die Finanzbetrugszahl durch synthetische Identitäten am schnellsten in den USA, und sie kostet Unternehmen jedes Jahr Milliarden von Dollar.

„Wir dürfen uns nicht mehr nur auf unsere Sinne verlassen, um digitale Identitäten zu überprüfen", erklärt Jonathan Daly, CMO von BioCatch. „Das KI-Zeitalter erfordert neue Methoden zur Authentifizierung. Bei unserer Arbeit haben wir gesehen, dass wir Signale der Verhaltensintention nutzen sollten. Dieser Ansatz hilft Finanzinstituten dabei, Deepfakes und Stimmklone in Echtzeit zu erkennen. Und so lässt sich das hart verdiente Geld der Kunden besser schützen."

www.biocatch.com

Testdatenmanagement

AUTOMATISIERUNG VON TESTDATEN-JOBS IN MICROSOFT AZURE DEVOPS-PIPELINES

– TEIL 4 VON 5 –

Diese fünfteilige Artikel-Reihe erkundet das Thema Testdatenmanagement (TDM), welches eine bedeutende Rolle in der Sicherstellung der Qualität von Softwareprodukten einnimmt. Die Serie beleuchtet verschiedene Facetten des TDMs, einschließlich bewährter Methoden, Herausforderungen und innovativer Lösungsansätze.

Um das Verhalten einer Anwendung während des Produktionsbetriebs genau zu bewerten, benötigen Entwickler eine Testumgebung, die der endgültigen Produktionsumgebung möglichst ähnlich ist. Allerdings kann eine Testumgebung niemals das gleiche Sicherheitsniveau wie die finale Produktionsumgebung erreichen. Dies stellt ein Dilemma dar, wenn es darum geht, Testdaten zu generieren und später im Testprozess zu verwenden. Tester stehen vor der Entscheidung, ob sie eine Kopie bereinigter Produktionsdaten verwenden oder möglichst realistische synthetische Testdaten erstellen sollen.

TDM umfasst diverse Aufgaben wie die Bereitstellung von Testdaten, Anonymisierung und Maskierung sensibler Daten, die Erstellung von Teilmengen (Subsetting), die Gewährleistung von Datenkonsistenz sowie die Integration in CI/CD-Pipelines. Eine effektive TDM-Strategie trägt zur Verbesserung der Softwarequalität bei, indem sie Tests unter realistischen Bedingungen ermöglicht, potenzielle Probleme frühzeitig aufdeckt und die Effizienz von Testprozessen steigert.

Die Artikelserie hebt die TDM-Funktionen von IRI Voracity hervor, eine Plattform für End-to-End Datenmanagement, die Datenerkennung, -integration, -migration und -verwaltung in einem Metadaten-Framework vereint. Die Nutzung von IRI Voracity ermöglicht eine effiziente Handhabung und führt zu Kosteneinsparungen in vernetzten IT-Umgebungen.

Azure DevOps-Pipeline

Dieser Artikel beschreibt, wie Testdaten-Jobs in einer Azure DevOps-Pipeline automatisiert werden, um realistische Testdaten für CI/CD zu erzeugen und zu nutzen. Mithilfe von SSH können Jobskripte oder API-Routinen direkt in der Pipeline ausgeführt werden. Das Backend bietet ausführbare Dateien für Sicherheitsfunktionen, und eine API kann auf vordefinierten Datenquellen arbeiten. Ein Docker-Image für die DevOps-Pipeline ist ebenfalls verfügbar.

Über Microsoft Azure Pipelines: Azure Pipelines ist eine Komponente der Azure DevOps-Suite, die eine Plattform für Continuous Integration und Continuous Delivery (CI/CD) bereitstellt. Sie ermöglicht es Entwicklern, automatisierte Prozesse für den Build, Test und die Bereitstellung ihrer Anwendungen einzurichten und auszuführen. Durch die kontinuierliche Integration und Bereitstellung von Codeänderungen können Entwickler ihre Softwareentwicklung beschleunigen und die Qualität ihrer Anwendungen verbessern. Azure Pipelines bietet eine Vielzahl von Funktionen, darunter Unterstützung für verschiedene Programmiersprachen, Integrationen mit bekannten Entwicklertools und die Möglichkeit, Builds auf verschiedenen Plattformen und Infrastrukturen auszuführen.

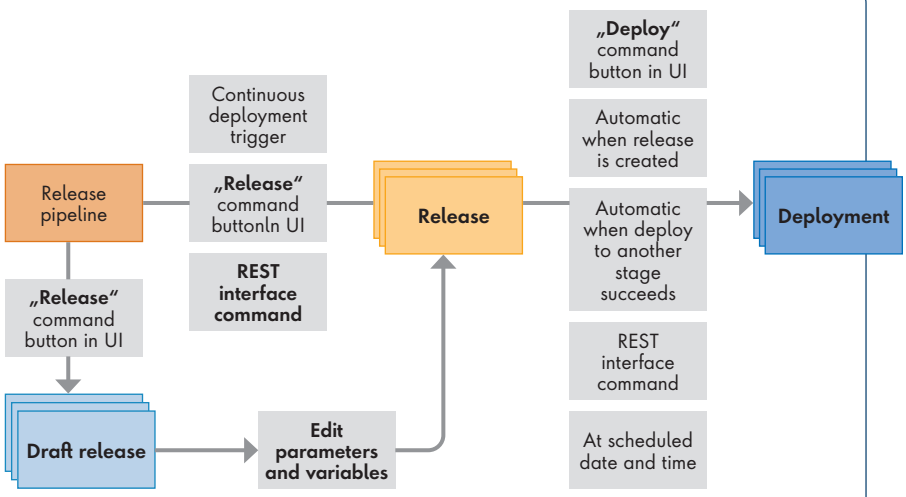


Bild 1: Verhältnis zwischen Veröffentlichungen, Releasepipelines und Bereitstellungen

Im Rahmen von DevOps spielt das Testdatenmanagement eine wichtige Rolle, da es verschiedene Tests im Entwicklungsprozess unterstützt, darunter automatisierte End-to-End- und Regressionstests, Produktions- und explorative Tests. Eine gute Testdatenverwaltung gewährleistet, dass Tests unter realistischen Bedingungen durchgeführt werden können und potenzielle Probleme frühzeitig erkannt werden können.

IRI Voracity bietet hierfür effiziente Lösungen, um unerwartete Fehler in der Produktionsumgebung zu vermeiden. Testumgebungen haben oft nicht dasselbe Sicherheitsniveau wie die Produktionsumgebung, weshalb direkte Tests mit Produktionsdaten riskant sind. Die Wahl zwischen maskierten Produktionsdaten und synthetischen Testdaten ist daher entscheidend.

Releases in Azure Pipelines

Eine Veröffentlichung in Azure Pipelines ist ein strukturiertes Konstrukt, das einen versionierten Satz von Artefakten enthält, die in einer CI/CD-Pipeline definiert sind. Sie umfasst alle erforderlichen Informationen für die Ausführung von Aufgaben und Aktionen in der Releasepipeline, wie Phasen, Aufgaben, Trigger und Bereitstellungsoptionen. Eine Releasepipeline kann mehrere Veröffentlichungen enthalten, und die Informationen werden für einen festgelegten Zeitraum gespeichert und angezeigt.

Eine Bereitstellung ist die Ausführung der Aufgaben für eine Phase, die automatisierte Tests, das Bereitstellen von Buildartefakten und andere Aktionen umfassen kann. Jede Bereitstellung wird gemäß den Einstellungen und Richtlinien gestartet, die in der ursprünglichen Releasepipeline festgelegt wurden. Es können mehrere Bereitstellungen pro Veröffentlichung durchgeführt werden, selbst in einer einzigen Phase. Wenn eine Bereitstellung fehlschlägt, kann die Veröffentlichung erneut in derselben Phase bereitgestellt werden.

TESTUMGEBUNGEN HABEN OFT NICHT DASSELBE SICHERHEITSNIVEAU WIE DIE PRODUKTIONSUMGEBUNG, WESHALB DIREKTE TESTS MIT PRODUKTIONSDATEN RISKANT SIND.

Amadeus Thomas, Geschäftsführer, JET-Software GmbH, www.jet-software.com

Möglichkeit einer SSH-Verbindung: Als Ergebnis der erfolgreichen Ausführung von SSH-Befehlen wird die entfernte Zielmaschine eine Batch-Datei ausführen, die die Testdaten-Jobs enthält, um bspw. sichere Testdaten in ein Excel-Blatt zu senden. Hier können Set-Dateien verwendet werden, um Testdaten zufällig auszuwählen und in eine Tabellenkalkulation zu integrieren. Set-Dateien sind ASCII-Wertelisten (die ähnliche Objekte enthalten), wobei jeder Wert in der Datei in einer neuen Zeile steht. Die Konfiguration der SSH-Aufgabe umfasst die Auswahl der SSH-Dienstverbindung und die Festlegung der auszuführenden Befehle.

Nach der Konfiguration der SSH-Aufgabe kann die Freigabepipeline bereitgestellt werden. Bei erfolgreicher Ausführung werden die SSH-Befehle auf der Remote-Maschine ausgeführt, wodurch eine Batch-Datei mit den Testdaten-Jobs aktiviert wird. Die Ergebnisse zeigen eine Excel-Tabelle mit zufällig generierten Testdaten. Zusätzlich (oder stattdessen) können auch andere Dateien oder Tabellen in relationalen Datenbanken erstellt werden, wie Microsoft SQL, MySQL, PostgreSQL, DB2 oder Oracle.

Bild 3: Ungeschützte persönlich identifizierbare Informationen (PII) in einem Eintrag

Bild 4: Durch den API-Aufruf, werden der Name, die E-Mail-Adresse und die SSN geschützt.

	A	B	C	D	E	F
1	1	Hesham	Purewal	manuals@verizon.net	215-419-7912	475678808
2	2	Batrina	Teng	marioph@outlook.com	973-847-2542	585432114
3	3	Zimmie	Ruckriegel	kohlis@mac.com	419-955-7418	525214818
4	4	Kenedra	Laterra	nelson@mac.com	313-346-6391	508675450
5	5	Shevin	Palus	sharon@verizon.net	480-389-1369	819678292
6	6	Tamron	Drechsler	dmiller@gmail.com	505-397-0176	190511462
7	7	Shang	Krentzman	dmbkiwi@outlook.com	440-752-4564	802824858
8	8	Vermont	Taps	muzzy@optonline.net	262-388-3779	605386449
9	9	Jenibelle	Oleske	dmiller@comcast.net	830-623-3192	435907207
10	10	Shirlette	Ritzer	agapow@att.net	903-803-6852	281719027
11	11	Ernest	Huggs	janneh@sbcglobal.net	307-777-0474	715724774
12	12	Urja	Kendal	loscar@outlook.com	925-660-1555	123140329
13	13	Amberlyn	Rehan	muzzy@att.net	661-938-5047	412515331
14	14	Meredith	Stukenberg	horrocks@comcast.net	478-692-0729	402448281
15	15	Ayari	Stellingwerf	amaranth@live.com	419-326-0783	355031033
16	16	Lucious	Jandres	falcao@outlook.com	707-287-4004	793293641
17	17	Shahzaib	Pasowicz	chaffar@yahoo.com	205-875-4021	765759320
18	18	Kiany	Uffelman	paulv@icloud.com	209-447-3939	629438174
19	19	Iciss	Hartnagle	redingtn@att.net	415-978-8113	684457453
20	20	Giuseppina	Pallman	hager@att.net	775-206-1986	733970965

Bild 2: Verwendung von Set-Dateien (ASCII-Wertelisten), um sichere Testdaten zufällig zu generieren

Fazit

IRI Voracity bietet eine ganzheitliche Lösung für die Automatisierung von Testprozessen und die Generierung individueller Testdaten aus verschiedenen Quellen. Mit IRI Voracity können Testdaten effizient bereitgestellt werden, was die Erstellung von Datenbanken mit referenzieller Integrität und die Simulation unterschiedlicher Datenformate ermöglicht. Da der Backend-Motor als ausführbares Programm konzipiert ist, kann IRI Voracity direkt von der Befehlszeile aus gesteuert werden. Durch die Integration von Voracity in den CI/CD-Prozess wird eine nahtlose Automatisierung von Aufgaben wie der Erzeugung synthetischer Testdaten oder der Maskierung sensibler Daten ermöglicht.

Amadeus Thomas

Alternativ dazu kann die Datenschutz-API programmgesteuert auf Datenquellen verwendet werden, um sensible Daten zu maskieren und in einen zweiten Datensilo für Tests zu schreiben. Nachdem der SSH-Befehl ausgeführt wird, werden Daten aus einem Produktionscontainer gelesen. Anschließend werden die sensiblen Daten unter Verwendung des Such- und Maskierungskontexts der API bereinigt und die maskierten Ergebnisse in einen zweiten Container geschrieben, der für Tests verwendet wird.

AUSBLICK

Im Abschluss dieser Serie wird demonstriert, wie man sichere Testdaten für CI/CD-Umgebungen in Jenkins einbindet.
Es wird beschrieben, wie Jenkins in einer virtuellen Maschine der Google Cloud Plattform gehostet und Subsetting-Jobs ausgeführt werden, um kleine aber präzise Datenbankkopien für Testzwecke zu erstellen.

CLEAN ARCHITECTURE PRAXISBUCH

FÜR SAUBERE SOFTWARE-ARCHITEKTUR UND WARTBAREN CODE

Eine wartungsfreundliche Architektur ist der Schlüssel, um Entwicklungsaufwand und -kosten niedrig zu halten. Dieses Buch vermittelt Ihnen alle notwendigen Fähigkeiten und Kenntnisse, um wartbare und langlebige Software zu entwickeln, ohne Vorkenntnisse vorauszusetzen.

Domänen-zentrierte Architektur in der Praxis

Dieser umfassende Leitfaden zeigt die Vorteile domänen-zentrierter Softwarearchitektur auf – angelehnt an Robert C. Martins Clean Architecture und Alistair Cockburns hexagonale Architektur. Anhand zahlreicher Beispiele erfahren Sie, wie Sie eine hexagonale Architektur in Ihrem Code abbilden können. Sie lernen verschiedene Strategien für das Mapping zwischen den Schichten einer hexagonalen Architektur kennen und erfahren, wie Sie die Architekturelemente zu einer Anwendung zusammensetzen.

Komplexe Konzepte leicht verständlich erklärt

Mit anschaulichen Erläuterungen und anhand zahlreicher Codebeispiele schafft dieses Buch ein tiefes und praxistaugliches Verständnis des hexagonalen Architekturstils. So sind Sie perfekt darauf vorbereitet, wartbare Anwendungen zu erstellen, die Zeit und Geld sparen.

Clean Architecture Praxisbuch - Für saubere Software-Architektur und wartbaren Code; Tom Hombergs; mitp Verlags GmbH & Co.KG; 05-2024

Continuous Controls Monitoring

MIT CCM DEN HERAUSFORDERUNGEN DER CYBERSICHERHEIT BEGEGNEN

In einer sich rasant entwickelnden Technologielandschaft sehen sich Unternehmen mit immer neuen Herausforderungen im Umgang mit potenziellen Sicherheitsrisiken konfrontiert. In diesem hochdynamischen Prozess wird die kontinuierliche Überwachung - Continuous Controls Monitoring (CCM) - zu einem Schlüsselprozess für die Resilienz und Effizienz innerhalb des gesamten Unternehmens. CCM bietet einen proaktiven und dynamischen Ansatz für das Risikomanagement, von der Alarmierung über Bedrohungen in Echtzeit bis hin zur automatischen Überwachung der Compliance.

Die Kontrolle von Zugriffen auf geschäftskritische Anwendungen dient Unternehmen dazu, ihre IT-Systeme vor unberechtigten Zugriffen, Datenverletzungen und anderen Sicherheitsbedrohungen zu schützen. Ziel der Kontrollen ist es unter anderem, die Nutzung von Softwareanwendungen auf Basis vordefinierter Richtlinien und Regelwerke wie dem BSI-Grundschutz, dem DSAG-Leitfaden und anderen GRC-Leitfäden zu überwachen, um sicherzustellen, dass Anwender nur autorisierte und vertrauenswürdige Business-Applikationen ausführen können. Dadurch wird das Risiko von Malware und anderen Sicherheitsvorfällen signifikant reduziert.

Herausforderungen der klassischen Kontrollmechanismen

Die übliche Methode zur Überwachung von Business-Applikationen ist ein auf Ausnahmen basierender Ansatz, bei dem Unternehmen einen vordefinierten Kontrollrahmen einrichten, um beispielsweise nicht autorisierte Änderungen von Stamm- und Bewegungsdaten oder auch Funktionstrennungskonflikte zu beobachten. Dabei muss die Evaluierung bislang weitgehend manuell gesteuert werden, was nicht nur hochqualifizierte IT-Ressourcen bindet, sondern nicht zuletzt auch viel Zeit kostet.

Hinzu kommt die Herausforderung, die generierten Reports, etwa zu Auffälligkeiten bei den Zugriffsrechten, richtig zu interpretieren und daraus sinnvolle Maßnahmen abzuleiten – hieran scheitern zuständige Fachabteilungen oftmals. Auf konventionellem Weg ist dies für Nicht-IT-Fachleute nur mit großem Aufwand und hoher Expertise zu bewerkstelligen, insbesondere bei der rasant wachsenden Anzahl von Applikationen.

Continuous Controls Monitoring

Hier setzt CCM an, indem es all diese Prozesse harmonisiert, und in einem klar

definierten gemeinsamen Regelwerk abbildet. CCM kann dabei eine Vielzahl von Regelwerken vereinheitlichen, so dass ein stabiles Fundament für das gesamte Unternehmen entsteht. Wichtig ist hierbei, die Qualität und den Reifegrad der einzelnen Regelwerke zu berücksichtigen und ein Gesamtregelwerk aufzubauen, das transparent und anpassbar ist und so die individuellen Anforderungen eines Unternehmens abbilden kann. Ist ein Regelwerk zu standardisiert und rudimentär, sind es zwangsläufig auch die späteren Ergebnisse.

Bei diesem dynamischen und proaktiven Ansatz werden automatisierte Prüfwerkzeuge eingesetzt, um die Kontrollen in Echtzeit zu überwachen und zeitgleich zu validieren. Im Gegensatz zur traditionellen periodischen Anwendungskontrolle gewährleistet die kontinuierliche Überwachung eine vollumfängliche Überprüfung, wobei Algorithmen zur schnellen Analyse großer Datenmengen eingesetzt werden, die eine sofortige und automatische Erkennung von Anomalien oder Auffälligkeiten ermöglichen, was zu einer erheblichen Risikominderung führt.

Insbesondere ist zu beachten, dass unternehmenskritische Applikationen nicht mehr rein SAP-immanent sind. Durch cloudbasierte Strukturen entstehen parallel zur altbekannten SAP-Welt neue und andere Risiken, denen auch andere Sicherheitsmechanismen folgen müssen. Wichtig ist daher, dass es den neuen Prozessen auch in dieser Hinsicht gelingt, alle unternehmensweiten Regelwerke zu harmonisieren und dies über die zunehmend verteilte Applikationslandschaft hinweg. Gerade vor dem Hintergrund von NIS2, der überarbeiteten EU-Richtlinie für Cybersicherheitsmaßnahmen, ist es von großer Bedeutung, einem Revisor jederzeit nachweisen zu können, welche Prozesse und Tools bereits implementiert sind und wie es um das Risikomanagement zur Stärkung der Netz- und Informationssicherheit bestellt ist.

> CCM BIETET EINEN PROAKTIVEN UND DYNAMISCHEN ANSATZ FÜR DAS RISIKO-MANAGEMENT, VON DER ALARMIERUNG ÜBER BEDROHUNGEN IN ECHTZEIT BIS HIN ZUR AUTOMATISCHEN ÜBERWACHUNG DER COMPLIANCE.
>
> **Ralf Kempf, Geschäftsführer, Pathlock Deutschland, www.pathlock.de**

Umfassende Kontrolle in Echtzeit

Entscheidend, auch für die regulatorischen Anforderungen von NIS2, ist, dass dies alles in Echtzeit geschieht. Nur so können kritische Situationen jederzeit ad hoc nachvollzogen und bewertet werden, ob damit ein signifikantes Risiko verbunden ist. Diese Prozesse im Continuous Controls Monitoring sind aufgrund ihres Automatisierungsgrades sehr ressourcenneutral. Ein Fachbereich wird jederzeit mit den relevanten Informationen versorgt und die bisherigen stichpunktartigen, oft manuellen Audits werden obsolet.

Der Schlüssel liegt darin, dass mit einem gut implementierten CCM-Tool stets aktuelle, auch für Nicht-IT-Experten verständliche Reports zur Verfügung stehen, die jedes Risiko konkret bewerten und klare Handlungsanweisungen an den Fachbereich geben. Das Pathlock Continuous Controls Monitoring visualisiert darüber hinaus beispielsweise den Sicherheitsstatus in Form von maßgeschneiderten Dashboards, etwa für die Managementebene. So wird dem CISO oder CFO prägnant und im angemessenen Detaillierungsgrad veranschaulicht, welche konkreten Findings aktuell für welchen Fachbereich vorliegen und welche Handlungsmöglichkeiten es gibt.

Risikoquantifizierung

Gerade für das C-Level ist die Risikobewertung durch Quantifizierung sehr interessant, da sie aufzeigt, welche finanziellen Auswirkungen eine kritische Situation auf das Gesamtsystem hätte. Dies geschieht im Pathlock CCM beispielsweise durch die Zuordnung von Kennzahlen im editierbaren Regelwerk. Wenn ein Risiko monetär beziffert wird, ob es potenzielle Verluste im zwei- oder sechsstelligen Eurobereich nach sich ziehen könnte, hilft das nicht nur dem CFO. Risiken konkret einschätzen zu können, die Reihenfolge der notwendigen Maßnahmen zu priorisieren und gegebenenfalls sehr schnell zu reagieren, ist immanent wichtig, da die Reaktionsgeschwindigkeit in Risikosituationen der entscheidende Faktor ist.

Die Zentralisierung kontinuierlicher Überwachung

Ein fortschrittliches Continuous Controls Monitoring bietet Unternehmen eine intelligente Kombination von Funktionen in einer integrierten Oberfläche, die die individuellen Kontroll- und Risikomanagementanforderungen von IT, HR, Finance und Audit unterstützt - und damit das Risikomanagement kosteneffizient orchestriert, Prozesse verbessert, gesetzliche Anforderungen erfüllt, Compliance nachweist und Risiken quantifiziert.

So zentralisiert die kontinuierliche Überwachung mit einem CCM-Tool die Analyse und Berichterstattung interner Kontrollen und fügt sich als integraler Bestandteil der Risikomanagement-Strategie nahtlos in die täglichen Geschäftsabläufe ein. Effizienz und Reaktionsfähigkeit bieten ein höchst anpassungsfähiges und effektives Mittel zur Aufrechterhaltung der Sicherheit und Integrität der Unternehmensprozesse.

Ralf Kempf

Die Informationsflut unter Kontrolle bringen

PROZESSE DIGITALISIEREN, DAS GESCHÄFT BESCHLEUNIGEN

Die Digitalisierung von Geschäftsprozessen eröffnet unzählige Möglichkeiten für mehr Effizienz im Unternehmen. Wer Papierstapel und Umlaufmappen beseitigt, beschleunigt sein Business und steigert seine Wettbewerbsfähigkeit. Digitale Dokumentenmanagement-Lösungen sind das Tool, das den Zugriff auf Informationen zur richtigen Zeit und am richtigen Ort ermöglicht.

Die meisten Unternehmen haben nach wie vor mit einem hohen Papieraufkommen zu kämpfen. Rechnungen, Dienstpläne oder Angebote werden in Papierform verschickt und stapeln sich. Zudem hat sich die E-Mail als wichtigster Kommunikationskanal etabliert. E-Mails enthalten Kundenanfragen, Bestellungen, angehängte Rechnungen als PDF oder unternehmensinterne Anliegen. All diese Informationen sind wichtig, aber das Sichten, Priorisieren und Zuordnen ist mit einem hohen Zeitaufwand verbunden. Im schlimmsten Fall bleiben wichtige Anfragen tagelang liegen oder werden doppelt bearbeitet.

Die gute Nachricht: Es gibt einen Ausweg aus diesem Dilemma. Durch die Digitalisierung von Geschäftsprozessen kann die Informationsflut in übersichtlichere Bahnen gelenkt werden. Ein Dokumentenmanagement-System, kurz DMS, ist dafür das geeignete Werkzeug. Es ermöglicht das schnelle Finden von Informationen, vereinfacht tägliche, zeitraubende Aufgaben und erhöht die Auskunftsfähigkeit gegenüber Kunden massiv.

UNTERNEHMEN MIT VIELEN PAPIERBASIERTEN PROZESSEN SOLLTEN NICHT LÄNGER WARTEN UND EIN DIGITALES DOKUMENTENMANAGEMENT-SYSTEM NUTZEN.

Dietmar Nick, CEO,
Kyocera Document Solutions Deutschland,
www.kyoceradocumentsolutions.de

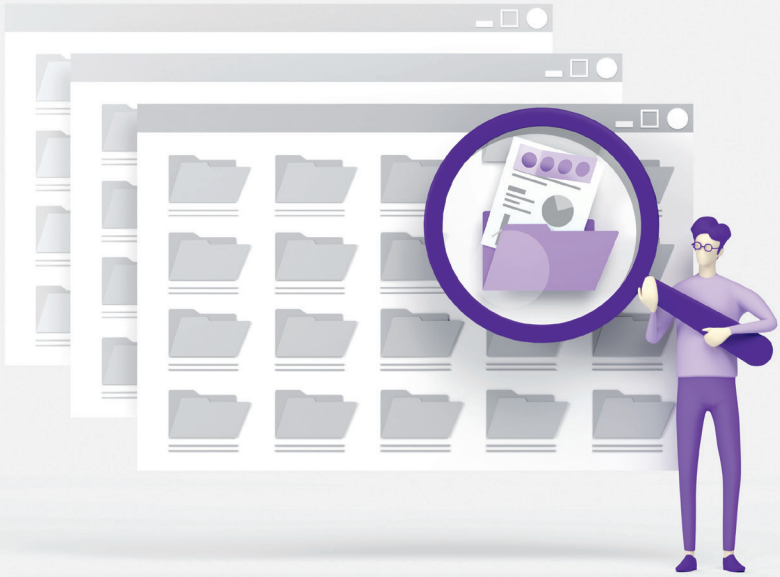
Risiken und Vorteile sorgfältig abwägen

Die Digitalisierung von Abläufen und Prozessen ist für viele Unternehmen ein wichtiges Thema. Dennoch zögern sie oft lange, bevor sie den Startschuss geben. Die Gründe hierfür sind vielfältig. Zum einen spielen die Kosten eine Rolle. Viele Unternehmen sind unsicher, ob sich die Investition in eine DMS-Lösung unter dem Strich wirklich lohnt. Bewährtes erscheint als vermeintlich sichere Bank mit kalkulierbaren Risiken. Hinzu kommt der Aufwand, der für viele Entscheider nur schwer sicher kalkulierbar ist. Die Einführung einer Dokumentenmanagement-Lösung ist immer ein IT-Projekt, das personelle und zeitliche Ressourcen bindet. Die erheblichen Chancen, die ein digitales Dokumentenmanagement für das Unternehmenswachstum und die Wettbewerbsfähigkeit bietet, werden dabei oft übersehen.

Diese Chancen sind technischer, personeller und wirtschaftlicher Natur. Technisch gesehen speichert eine Dokumentenmanagement-Lösung Dokumente in einer zentralen Datenbank und macht jede benötigte Information in Sekundenschnelle auffindbar. Ein Berechtigungsmanagement stellt sicher, dass nur autorisierte Mitarbeitende Zugriff auf vertrauliche Dokumente haben.

Alle Mitarbeitenden arbeiten automatisch immer mit der aktuellsten Version eines Dokuments. Bei jeder Änderung eines Dokuments wird eine neue Version abgelegt. So ist sichergestellt, dass alle Nutzerinnen und Nutzer immer über den aktuellen Kenntnisstand verfügen und eine Bearbeitung einer alten Datei oder Vorlage vermieden wird.

Bei der Auswahl einer DMS-Lösung ist die einfache Implementierung und Nut-



zerführung ein entscheidender Faktor. Die Integration in bestehende Anwendungen und Prozesse ist dabei von großer Bedeutung. Ein Beispiel hierfür ist die Integration in Microsoft Office. Die digitale Dokumentenmanagement-Lösung Kyocera Workflow Manager bietet beispielsweise eine nahtlose Integration in die Office-Welt. Die reine Installation der Lösung dauert nur wenige Stunden. Das modulare Konzept ermöglicht es auch weniger IT-affinen Anwenderinnen und Anwendern, schnell mit der Software zu arbeiten. Der Schulungsaufwand ist gering, was die Akzeptanz in der Belegschaft erhöht.

Digitalisierung braucht Akzeptanz

Akzeptanz ist ohnehin ein entscheidender Faktor. Bei der Einführung von Dokumentenmanagement-Systemen sollte mit wirkungsstarken Prozessen wie dem Rechnungseingang begonnen werden, bei denen der Mehrwert direkt ersichtlich ist. Nach erfolgreicher Einführung wird die DMS-Lösung dann schrittweise in anderen Bereichen implementiert, um einen abrupten Umbruch zu vermeiden. Dieses schrittweise Vorgehen fördert die Gewöhnung an die neuen Prozesse und die Akzeptanz in den Teams.

Ein digitales Dokumentenmanagement-System verbessert die Zusammenarbeit im Team erheblich. Digitale Freigabeprozesse beschleunigen die Arbeitsabläufe und eliminieren repetitive Aufgaben wie die Suche nach Dokumenten. Zudem wird wichtiges Wissen, das bisher in den Köpfen einzelner Mitarbeitender oder in physischen Ordnern verborgen war, zentralisiert und jederzeit abrufbar. Dieses Wissen bleibt auch bei Personalwechseln erhalten und kann zur Prozessoptimierung und Neukundengewinnung genutzt werden.

Eine erfolgreiche DMS-Implementierung führt zu einer Steigerung der Produktivität. Anwenderberichte bestätigen eine deutliche Zeitersparnis, die in die Bearbeitung anspruchsvollerer Aufgaben investiert werden kann. Der Mehrwert ist nicht nur intern, sondern auch extern spürbar. Die Kunden profitieren von einer schnelleren und effizienteren Bearbeitung ihrer Anliegen durch das Unternehmen.

Rechtssicher archivieren

Digitales Dokumentenmanagement schützt Unternehmen auch vor rechtlichen Risiken. Nach den „Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" (GoBD) müssen steuerrelevante Dokumente nach bestimmten Kriterien archiviert werden.

Moderne DMS-Lösungen gewährleisten daher die Erfüllung aller gesetzlichen Anforderungen an Datensicherheit und Datenintegrität, einschließlich einer GoBD-konformen Archivierung. Bei Ablauf der gesetzlichen Aufbewahrungsfristen unterstützt das System durch automatische Erinnerungen an Löschfristen, so dass nicht mehr benötigte Dokumente einfach entfernt werden können.

Darüber hinaus erleichtert ein DMS Betriebsprüfungen, da alle relevanten Dokumente schnell verfügbar sind. Die Einhaltung der GoBD-Vorschriften kann durch eine entsprechende Verfahrensdokumentation zuverlässig nachgewiesen werden, was den Prüfungsprozess beschleunigt.

On-Premises oder Cloud?

Unternehmen können bei der Einführung einer DMS-Lösung zwischen cloudbasierten und On-Premises-Lösungen wählen. Letztere erfordern zwar häufig eine höhere Anfangsinvestition und die laufende Wartung durch eigene IT-Spezialisten, ermöglichen aber die volle Kontrolle über alle Informationen und die Server, auf denen sie archiviert werden. Cloud-Lösungen wie der Kyocera Cloud Information Manager hingegen sind besser skalierbar und belasten die IT-Ressourcen des Unternehmens deutlich weniger. Wartung und Updates des Systems werden vom Anbieter übernommen.

Die Entscheidung zwischen einer Cloud- und einer On-Premises-Lösung hängt letztlich von den individuellen Anforderungen und Ressourcen eines Unternehmens ab. Die Cloud stellt jedoch eine moderne, flexible und kostengünstige Alternative dar, die den heutigen Anforderungen an Mobilität und Flexibilität gerecht wird.

Unternehmen mit vielen papierbasierten Prozessen sollten nicht länger warten und ein digitales Dokumentenmanagement-System nutzen, um ein effektives Wissensmanagement im Unternehmen aufzubauen, ihre Innovationskraft zu stärken und ihre Wettbewerbsposition zu verbessern.

Dietmar Nick

Effektives Cloud Cost Management

WARUM FINOPS ALS BASIS UNVERZICHTBAR SIND

Über eine Billion US-Dollar sollen die Ausgaben für Public Clouds im Jahr 2026 erreichen, so die aktuelle Prognose des US-Analystenhauses Forrester. Das sind fast 50 Prozent mehr als die Kosten, die von Gartner für dieses Jahr errechnet wurden. Trotz dieses dynamischen Wachstums haben die meisten Unternehmen nach wie vor keine Transparenz über die detaillierten Kosten für ihre Cloud-Ressourcen. Die Folgen sind durch viele Untersuchungen und Studien gut belegt: In der Praxis liegen die unnötigen Mehrausgaben bei bis zu einem Drittel oder gut 200 Milliarden Euro. Zum Beispiel gaben 72 Prozent der von Forrester gefragten IT-Entscheidungsträger an, dass sie ihr Cloud-Budget im letzten Geschäftsjahr überschritten haben. Übermäßige Ressourcennutzung, unvorhergesehene Kostenfaktoren und ineffektives Kostenmanagement spielen hier zusammen. Die Tatsache, dass immer mehr Teams und Funktionen in Unternehmen die Verantwortung für Cloud-Kosten haben, erschwert die Sichtbarkeit dieser Kosten im Sinne einer konsolidierten Übersicht zusätzlich.

Viele Daten, wenig Klarheit und Zuordnung

Rechnungen von Cloud-Providern wie AWS, Google Cloud Platform oder Microsoft Azure werden aufgrund ihrer Komplexität und Detaillierung oft als intransparent empfunden. Aufgelistet werden etwa die Kosten für verschiedene Instanztypen je nach Konfiguration (CPU, Speicher, etc.) und Region, die Gebühren für verschiedene Speicherdienste wie Objektspeicher (zum Beispiel S3 bei AWS), Blockspeicher und Dateispeicher, die Aufwände für Datenübertragung oder Datenbankdienste sowie weitere Service-spezifische Gebühren, zum Beispiel für die Nutzung von APIs oder zusätzliche Dienste, etwa für Machine Learning-Services etc. Die Vielzahl der Service-Optionen und deren unterschiedliche Preisgestaltungen machen es schwierig, den genauen Ursprung der Kosten zu identifizieren. Oft werden Kosten für verschiedene Ressourcen und Dienste als Sammelrechnung zusammengefasst dargestellt, ohne dass eine detaillierte Aufschlüsselung pro Projekt oder Abteilung erfolgt, was die interne Kostenzuordnung erschwert. In diesem Fall hilft ein detailliertes Tagging von Ressourcen, die Kosten spezifischen Teams, Projekten oder Diensten zuzuordnen.

Mit FinOps die Cloud-Nutzung optimieren

Seit einiger Zeit versuchen IT-Verantwortliche, die Kostenspirale mit Financial Operations (FinOps) in den Griff zu bekommen. Die sich entwickelnde Disziplin und kulturelle Praxis des Cloud-Finanzmanagements umfasst die Implementierung von Prozessen, Tools und Richtlinien, die es Unternehmen ermöglichen, ihre Cloud-Ausgaben transparent zu machen, besser zu verwalten und zu optimieren. Dazu gehören die Nutzung von Kostenmanagement-Tools, die Themen wie Monitoring oder Software Asset Management integrieren, die Einführung klarer Kostenzuweisungen und Verantwortlichkeiten, die Automatisierung von Prozessen zur Kostenoptimierung sowie die Förderung einer Kultur der Kostenbewusstheit und Zusammenarbeit.

FinOps-Initiativen sind jedoch in der Praxis oft schwer umzusetzen, weil sie eine kulturelle und organisatorische Veränderung erfordern. Unternehmen müssen traditionelle Silos zwischen Finanz-, IT- und Geschäftsteams überwinden und ein gemeinsames Verständnis für Cloud-Kosten entwickeln. Die Integration von Finanz- und Operationsdaten beansprucht zudem Zeit und Ressourcen. Darüber hinaus kann der Mangel an Tools und Fachwissen die Implementierung erschweren. Daher entscheiden sich immer mehr Unternehmen für extern erbrachte FinOps Managed Services.

Typische Kostentreiber identifizieren

Ein zielführender Lösungsansatz von FinOps ist es, die häufigsten Kostentreiber zu identifizieren und zu verstehen, welche Kosten vermieden werden könnten und wie sie sich negativ auf das Budget auswirken. Wichtige Kostentreiber sind:

➤ **Überprovisionierung oder „schlafende" Instanzen:** Unternehmen neigen dazu, mehr Ressourcen zu erwerben als

nötig. Ohne transparente Übersicht können ungenutzte Ressourcen kontinuierlich Kosten verursachen.

➤ **Unvorhergesehene oder versteckte Kosten:** Unerwartete Kosten, besonders durch Datenübertragung, können die erwarteten Cloud-Rechnungen erheblich übersteigen.

➤ **Nicht ausgelastete Server:** Überwachung der Datennutzung und Serverauslastung ist wichtig, um ungenutzte Ressourcen zu identifizieren und entsprechend anzupassen oder zu veräußern.

➤ **Regionale Kostenunterschiede:** Die Preise für Cloud-Services variieren je nach Region. Durch Auswahl der richtigen Region können signifikante Einsparungen erzielt werden.

➤ **Auswahl von Instanztypen:** Die richtige Auswahl von Instanztypen ist wichtig, da leistungsfähigere Instanzen höhere Kosten verursachen. Reservierte Instanzen sollten sorgfältig geprüft und mit On-Demand-Optionen verglichen werden.

➤ **Compliance und Sicherheit:** Einhaltung von Compliance-Anforderungen und Sicherheitsmaßnahmen können zusätzliche Kosten verursachen, die überwacht und verwaltet werden müssen.

Um Cloud-Ausgaben nachhaltig zu reduzieren, ist es unerlässlich, diese Aspekte zu verstehen und effektive Strategien zur Kostenkontrolle zu implementieren. Laut einem Report des US-Datenanalyse-Unternehmens Anodot machen Daten- und Speicheroptimierungen etwa 80 Prozent der Einsparungen aus.

Konkrete Mehrwerte durch Cloud Cost Management

Das Erkennen von Nutzungsmustern und die Eliminierung ungenutzter Instanzen sind entscheidende Bestandteile eines Cloud Cost Managements. Unterstützt wird dieser Prozess durch Monitoring- und Alarmierungssysteme, die fortlaufend die Kapazitätsparameter der Cloud-Services überwachen. Diese Systeme melden automatisch, wenn Cloud-Systeme „betriebsbereit, aber ungenutzt" sind und schlagen Maßnahmen wie die Nutzung, den Wechsel zu kleineren Systemen oder das Beenden des Cloud-Services vor. Integrierte Eskalationsmechanismen gewährleisten, dass Kostenstellenverantwortliche informiert werden oder Systeme automatisch heruntergefahren werden. Zudem überwachen diese Systeme in Echtzeit die Einhaltung der SLAs für Cloud-Komponenten.

Eine effektive Methode ist auch die Identifizierung und Deaktivierung ungenutzter Konten durch Software Asset Management-Tools, was bei großen Unternehmen jährliche Einsparungen von bis zu 30 Prozent ermöglichen kann, zum Beispiel durch das Abschalten von MS 365-Abonnements. Die Anpassung der Abonnements entsprechend der tatsächlichen Nutzung ist ebenfalls kostensparend, da viele Nutzer teure Abonnements haben, jedoch nur Grundfunktionen benötigen, die durch günstigere Abonnements abgedeckt werden können.

Ein weiterer Ansatz für Kosteneinsparungen ist die Nutzung von „Bring Your Own License" (BYOL)-Rechten. Unternehmen, die ihre vorhandenen Oracle-On-Premises-Lizenzen in die Cloud übertragen, können ebenfalls über 30 Prozent ihrer jährlichen Lizenzkosten für SQL-Datenbanken sparen.

Diese Beispiele verdeutlichen, wie durch integrierte FinOps-Maßnahmen für Cloud Cost Management erhebliche Kosteneinsparungen realisiert werden können.

Dr. Thomas Gerick
www.usu.com

IT SERVICE MANAGEMENT 2024

WIE KI DAS ITSM VERÄNDERT UND HERAUSFORDERT

Je mehr KI-Anwendungen auf den Markt drängen, desto stärker werden IT-Teams in die Verantwortung gezogen. In Deutschland entscheiden 49 Prozent von ihnen in ihren Unternehmen (mit), welche KI-Tools und -Services eingeführt und genutzt werden. Für viele ist das allerdings keine leichte Aufgabe. Jedem Zehnten fehlt, dem zweiten Teil der aktuellen Studie „OTRS Spotlight: IT Service Management 2024" zufolge, ein Überblick über die vielen KI-Tools und -Services, deren Einsatzgebiete, potenziellen Nutzen, Kosten und Risiken. 43 Prozent haben zwar einen groben Überblick, finden es aber nicht immer einfach zu evaluieren, welche KI-Tools und -Services für ihr Unternehmen nützlich sein könnten. Hinzu kommt, dass viele IT-Teams mit Anfragen von Mitarbeitenden zu KI-Anwendungen und deren Nutzung überhäuft werden. Ein Drittel erhält praktisch täglich Fragen zu Funktionen und Anwendungsmöglichkeiten bestimmter KI-Tools oder -Services; weitere 34 Prozent mehrmals in der Woche. Für die Studie hat das Softwareunternehmen OTRS AG international 600 IT-Verantwortliche und -Mitarbeitende befragt, 100 davon in Deutschland.

KI-Richtlinien

Ein Mittel, um die IT-Teams zu entlasten, können Richtlinien für die Nutzung von KI-Tools und -Services im eigenen Unternehmen sein, an denen sich Mitarbeitende orientieren können. Solche Richtlinien gibt es bislang allerdings nur in der Hälfte der deutschen Unternehmen. Die Mehrheit der anderen Hälfte sieht aber offenbar dringenden Handlungsbedarf: 42 Prozent arbeiten aktuell an KI-Richtlinien. Nur 8 Prozent haben weder bereits Richtlinien, noch arbeiten sie derzeit daran.

Was vielen IT-Teams ebenso fehlt wie KI-Richtlinien, ist ein Überblick darüber, welche KI-Tools und -Services die Mitarbeitenden in ihrem Unternehmen bereits nutzen. 38 Prozent wissen nur zum Teil, welche das sind, vier Prozent haben keinerlei Überblick darüber.

Über die Anwendungsmöglichkeiten von KI in ihrem eigenen Arbeitsbereich – im IT Service Management (ITSM) – fühlt sich die Mehrheit der IT-Teams in Teilen gut informiert, findet es jedoch auch hier schwer, einen vollständigen Überblick zu erhalten (57 Prozent). 41 Prozent sind hingegen überzeugt, genau über die Anwendungsmöglichkeiten von KI im ITSM Bescheid zu wissen.

Leistung und Kundenzufriedenheit verbessern

Ungeachtet der zusätzlichen Arbeit, die für IT-Teams durch KI-Anwendungen anfällt, sind sie davon überzeugt, dass diese sowohl für ihr Unternehmen als auch für ihre eigene Arbeit von großem Nutzen sein kann. Hauptgrund für die Einführung von KI-Anwendungen in ihrem Unternehmen ist für die meisten, bessere Leistungen zu erzielen (64 Prozent). Für etwas mehr als die Hälfte (55 Prozent) zählt die Steigerung der Kundenzufriedenheit beziehungsweise die Verbesserung des Services zu den wichtigsten Gründen für die KI-Implementierung. Zeit- und Kostenersparnis stehen mit 46 und 41 Prozent an dritter und vierter Stelle der wichtigsten Gründe.

www.otrs.com

Gute Gründe für hybrid

GÜNSTIG, SICHER, NACHHALTIG

Die Ankündigung, dass Microsoft seine Office und Windows Server erneut für den on-premises-Gebrauch launcht, hat manchen IT-Verständigen überrascht. VENDOSOFT-CEO Björn Orth nicht. Sein Unternehmen handelt Microsoft-Lizenzen in allen Facetten: neu, gebraucht und aus der Cloud. Das Geschäft mit den Gebrauchten boomt, denn sie spielen eine zentrale Rolle in den hybriden Infrastrukturen, die er anstelle von ‚Cloud-only' empfiehlt.

Das Lizenzmanagement automatisieren

„Wir verhelfen Unternehmen und Behörden zu einer optimalen Lizenzierung – ohne die Abhängigkeit von überteuerten Abo-Diensten", erklärt der Microsoft-Fachmann die Beratungsleistung von VENDOSOFT. Oft hören seine Mitarbeitenden, ein Mix aus on-prem und Cloud mache das Lizenzmanagement komplizierter. Das stellt er in Relation zu den Vorteilen. „Im Vergleich zu reinen 365-Plänen sparen hybride Konstellationen mit Gebrauchtsoftware 30 bis 50 Prozent der jährlichen Cloud-Kosten ein. Dem steht ein überschaubarer Mehraufwand bei der Lizenzverwaltung gegenüber." Viele Kunden lösen das über Gruppenrichtlinien, die beispielsweise prüfen, ob die Programme eines Rechners aktualisiert werden müssen und die Installationen automatisiert ausführen. Ebenfalls praktisch: Gebrauchtsoftware-Käufe erfolgen über den Online-Shop oder persönliche Berater. Im Kundenportal werden automatisch alle Rechnungen, Lizenzdokumente und Produkt-Keys angezeigt.

Nachhaltigkeit im Lizenzmanagement

So günstig und kommod gebrauchte Microsoft-Lizenzen bei dem Reseller zu beschaffen sind, so nachhaltig ist es, sie zu nutzen. Denn die Lebensdauer von Software beeinflusst die Lebensdauer der Hardware, auf der sie läuft. Was im Fachjargon als „Softwarebedingte Obsoleszenz" bezeichnet wird, bedeutet, dass mit jedem Upgrade die Systemanforderungen steigen – oft um viele hundert Prozent. Das kann zu Konflikten führen. „Ein Feature der Cloud ist das automatische Upgrade auf die stets neueste Office- oder Server-Version" berichtet Björn Orth. Unerwünschter Nebeneffekt: Unternehmen werden gezwungen, immer neuere Computer, Tablets oder Server anzuschaffen. Auch refurbished Geräte können nur begrenzt mit Cloud-basierten Programmen genutzt werden. „Wem der CO_2-Footprint der IT wichtig sind, dem sei deshalb zu älteren Software-Versionen geraten." Erhältlich sind gebrauchte Betriebssysteme, Office-Pakete und Microsoft Server bei dem Anbieter in sämtlichen noch supporteten Versionen. Nachhaltiger geht es nicht.

EIN KOSTENBEWUSSTES LIZENZMANAGEMENT IST HEUTE HYBRID UND NUTZT DAS BESTE VON BEIDEM: DIE GÜNSTIGEN EINMALKOSTEN GEBRAUCHTER KAUF-SOFTWARE UND DIE VORTEILE FÜR REMOTE-WORK AUS DER CLOUD.

Björn Orth, Geschäftsführer, VENDOSOFT GmbH, www.vendosoft.de

Mit Gebrauchtsoftware zur Digitalisierung

Man könnte meinen, frühere Software-Versionen sind ein Hemmschuh bei der Digitalisierung. Tatsächlich jedoch begünstigt das eine das andere: Unternehmenskunden zahlen für gebrauchte Microsoft-Lizenzen signifikant weniger als für die vergleichbaren Online-Dienste. Sie zahlen on-premises zudem einmalig, nicht jährlich wiederkehrend. Wer bei der Microsoft-Lizenzierung Budgets im vielstelligen Bereich einspart, kann sie anderswo investieren. Und ist trotzdem optimal ausgestattet! Weil die meisten Office User nicht die neueste Version benötigen. Weil ein Terminal Server sicherer sein kann als sein Pendant aus der Cloud. Und weil sich nicht jedes Unternehmen die massiven Preissteigerungen leisten kann oder will, die Microsoft jährlich vornimmt.

Die (kostenlose) Lizenzberatung von VENDOSOFT zielt genau darauf ab: die bestmögliche und zugleich günstigste Lösung für den Kunden zu finden. Das können reine Kauflizenzen sein. Oft ist es jedoch der hybride Mix aus Cloud und Kauf-Software. Deshalb ist es laut Björn Orth gut, dass Office 2024 und Windows Server 2025 kommen. „Damit können wir Unternehmen weiterhin bezahlbare on-premises-basierte Lizenzierungen anbieten."

Angelika Mühleck | www.vendosoft.de

Effiziente Lizenzverwaltung

ZEIT UND KOSTEN SPAREN MIT SOFTWARE ASSET MANAGEMENT

Die Geschichte der Software-Entwicklung ist faszinierend – was vor rund 80 Jahren als mathematische Spielerei begann, ist heute die Grundlage für fast alles, was in der Wirtschaft vor sich geht. Tatsächlich verdiente lange Zeit der einst reichste Mensch der Welt, Microsoft Gründer Bill Gates, sein Vermögen durch den Verkauf von Software. Wobei das genau genommen nicht stimmt: Nicht die Software wird verkauft, sondern ihre Lizenz. Doch womit der eine viel Geld verdient, bedeutet für den anderen oft hohe Kosten. Wer hier nicht mehr Geld als unbedingt notwendig ausgeben möchte, muss sich mit dem Thema Lizenzmanagement auseinandersetzen.

Die händische Erfassung des aktuellen Softwarebestandes ist längst durch die reine Menge zu einer unlösbaren Sisyphus Aufgabe geworden. So besteht die Gefahr, dass installierte Anwendungen nicht erfasst werden. Das entspricht einer Unterlizensierung und damit einer unbefugten Nutzung. Das ist keine rein rechtliche Komponente. In den Lizenzverträgen sichern sich viele Hersteller in der sogenannten Prüfungsklausel das Recht zu, unangemeldete Audits durchzuführen. Weichen die Ergebnisse dieser Erhebungen vom gemeldeten Stand ab, kann das unangenehme Folgen für das Unternehmen haben. Ebenso können aber auch mehr Lizenzen als nötig vorhanden sein – eine Verschwendung des IT-Budgets. Dabei geht es um erhebliche Summen: Softwarelizenzen gehören mittlerweile zu den größten IT-Kostenfaktoren.

Software Asset Management bring Klarheit

Eine Lösung dafür bietet Software Asset Management (SAM). Es erlaubt Unternehmen, ihre Softwarelizenzen effizient zu verwalten und so rechtliche sowie finanzielle Risiken zu minimieren. Dabei besteht SAM aus mehreren Elementen:

- Inventory-Software bietet sich für die effiziente Erfassung des aktuellen Status an. Diese durchsucht automatisiert das eigene Netzwerk und erfasst installierte Anwendungen. Neben Bezeichnung registriert sie Produkt-ID, Installationsgröße und -pfad sowie Version.

SOFTWARE ASSET MANAGEMENT ERLAUBT UNTERNEHMEN, IHRE SOFTWARELIZENZEN EFFIZIENT ZU VERWALTEN UND SO RECHTLICHE SOWIE FINANZIELLE RISIKEN ZU MINIMIEREN.

Hanno Scheppig, Produkt Manager, baramundi software GmbH, www.baramundi.de

- Software Metering auch als Application Usage Tracking bezeichnet, hilft nur selten oder gar nicht genutzte Anwendungen aufzuspüren.
- Application Control ermöglicht über Berechtigungen zu steuern, wer bestimmte Software nutzen darf. Neben lizenzrechtlich korrekter Anwendung sorgt Application Control auch als Sicherheitsmaßnahme gegen den Zugriff unbefugter Personen.
- Request Management ist für die Interaktion mit den Anwendern zuständig. Es fungiert als zentrale Anlaufstelle für Softwarewünsche und spielt im Bereitstellungsprozess eine tragende Rolle.
- License Manager ist ein intelligentes Verzeichnis für Lizenzbedingungen, der für die eigentliche Lizenzprüfung verantwortlich ist. Er vergleicht die Daten des Software Inventory mit den verfügbaren Lizenzen, den Anforderungen des Lizenzgebers und verschafft eine Übersicht über den Ist-Zustand. Seine Lizenzverwaltung enthält Angaben über Lizenzdaten, Vertragsinformationen, Angaben zur Verwendung des Produktes, ein Dokumentenupload sowie Verknüpfungen zu Rahmenver-

trägen. Optional erfasst ein Product Catalog spezifische Informationen wie Name, Edition, Version oder die Vertragsart, die der Verwendung der Software zugrunde liegt. Diese Informationen können dann vereinheitlicht im SAM verwendet werden.

Akteure mit verschiedenen Interessen

Je nach Unternehmensgröße kann Software Asset Management eine ganze Reihe an Abteilungen betreffen:

1# **Systemadministration:** Hier liegt der Fokus auf der Unterstützung der Anwender und dem Betrieb der IT-Infrastruktur. Die eigentlichen Lizenzverträge sind hier nur selten relevant – lediglich die Anzahl verfügbarer Lizenzen.

2# **Lizenzmanagement:** Als Bindeglied zwischen IT und kaufmännischer Abteilung benötigten Lizenzmanager einen vollständigen Überblick zu allen Details.

3# **Einkauf:** Hier wird ein Lizenzmanagement mit klaren Berichten benötigt, ohne zu großen Detailreichtum und Komplexität, um die besten Vertragskonditionen zu erschaffen.

4# **Compliance und Top Management:** In diesem Bereich besteht das Interesse primär in der Einhaltung von Budget und Compliance-Vorgaben.

Um diese unterschiedlichen Interessen zu erfüllen, empfiehlt sich ein enger Austausch zwischen den unternehmensinternen Akteuren. Im Falle eines Audits ist ein externer SAM-Berater durch seine Erfahrung und Expertenwissen eine große Hilfe.

Fallstricke und Lösungen

Bei SAM gibt es eine Reihe möglicher Fallstricke, die es zu beachten gilt:

- Gewachsene Lizenzstrukturen
- Abhängigkeiten
- individuelle Lizenzmodelle, Editionen und Preise
- Komplexität einzelner Lizenz- und Vertragselemente (Lizenzierung pro Gerät, User, CPU)

Viele Lösungen sind deshalb sehr umfangreich und fokussieren sich auf die Lizenzmanager, bieten den Entscheidern in den jeweiligen anderen Abteilungen aber nur selten eine schnelle, einfache Übersicht.

Für viele Unternehmen wäre ein Mittelweg die bessere Wahl: Statt eines Feature-überladenen Systems oder der minimalistischen Verwaltung über Excel-Tabellen, ist eine leichtgewichtige, aber dennoch leistungsfähige Lösung vollkommen ausreichend. Wichtig ist vor allem, dass die Lösung, die im Software Asset Management erhobenen Daten, reibungslos weiterverarbeiten kann. Ausreichend Schnittstellen und Berichtsfunktionen sind daher das A und O. Natürlich müssen die Berichtsdaten auch nach Verwendungsart aufbereitet werden können – je nachdem, ob sie für eine Bilanz, Produkt- bzw. Lizenzübersicht, einen Bericht über die Lizenznutzung oder den Stand der aktuellen Verträge benötigt werden.

Ergebnisse durch SAM

Nach Prüfung der Situation kann SAM zu verschiedenen Ergebnissen führen:

- System ist in Compliance: Keine weiteren Schritte notwendig.
- Umstrukturierung von Hardware: CPUs, VMs, Benutzer, etc. müssen neu zugeteilt werden, um Lizenzen zu sparen.
- Eine alte Lizenz gilt auch für neue Versionen: Damit entfällt der Bedarf, gesondert Rechte zu erwerben.
- Bei Softwarewartungsverträgen liegt ein Überschuss vor: In diesem Fall können Entscheider aus dem Einkauf eine Reduzierung der nicht benötigten Wartung vornehmen.
- Software wird nicht genutzt: Ungenutzte Installationen können entfernt werden und so schnell eine bestehende Unterlizenzierung korrigieren.

Verbesserte Zusammenarbeit und Betriebsergebnis

Die Einführung eines effizienten, leichtgewichtigen Software Asset Managements kann helfen, die Zusammenarbeit der verschiedenen Akteure im Unternehmen zu verbessern, indem der Kenntnisstand aller Beteiligten unkompliziert auf das gleiche Niveau gebracht wird. Den größten Mehrwert bietet Software Asset Management, wenn es in Kombination mit einer plattformübergreifenden Unified-Endpoint-Management-Lösung eingesetzt wird. IT-Verantwortliche können so direkt und übersichtlich Aufgaben abarbeiten, die sich aus der jeweiligen Lizenzsituation ergeben. Das Unternehmen schafft Compliance und vermeidet unnötige Mehrarbeit sowie Ausgaben.

Hanno Scheppig

Versteckte IT-Ausgaben aufdecken

LIZENZMANAGEMENT-SOFTWARE ALS LÖSUNG

Lizenzmanagement und der Lizenz-Dschungel ist kein neues Thema, doch es bleibt hochaktuell. Haben Sie sich jemals gefragt, wie viel Geld Ihr Unternehmen durch ineffizientes Lizenzmanagement verliert? Dieser unsichtbare Geldfresser kann erhebliche Kosten verursachen. Eine effiziente Lizenzmanagement-Software kann helfen, diese Kosten zu senken und gleichzeitig die IT-Compliance zu gewährleisten.

Einfache Lösungen für komplexe Probleme

Egal, ob großer Konzern, kleines oder mittelständisches Unternehmen (KMU) oder öffentlicher Sektor – ineffizientes Lizenzmanagement betrifft jeden. Die zunehmende Komplexität von Lizenzmodellen, die Verbreitung von Cloud-Computing und die Verwaltung hybrider IT-Umgebungen machen Lizenzmanagement zu einer dauerhaften Herausforderung. Organisationen müssen ihre Strategien kontinuierlich anpassen, um rechtliche Risiken zu minimieren und Kosten zu optimieren.

Herausforderungen des Lizenzmanagements

Die hybride Software-Lizenzierungslandschaft und das Software Asset Management (SAM) durchlaufen einen entscheidenden Wandel, angetrieben durch die Einführung von Subscription-Modellen und SaaS-Angeboten. Diese Entwicklungen haben das Lizenzmanagement komplexer gemacht und erfordern eine beständige Anpassung der Abonnements sowie eine genaue Budgetplanung.

Lizenzmanagement als IT-Asset-Management-Strategie

Lizenzmanagement sollte nicht isoliert betrachtet werden, sondern als integraler Bestandteil einer umfassenden IT-Asset-Management-Praxis. IT-Asset-Management (ITAM) umfasst die Verwaltung aller IT-Ressourcen und ihrer Lebenszyklen, von der Beschaffung bis zur Entsorgung. Durch die Integration von Lizenzmanagement in ITAM können Unternehmen nicht nur ihre Softwarelizenzen effizient verwalten, sondern auch die Nutzung aller IT-Ressourcen optimieren. Eine leistungsstarke Softwareinventarisierung, die anzeigt, welche Software auf welchem Gerät installiert ist, ist dabei ein wesentlicher Bestandteil.

Lizenz-Dschungel: IT-Budget unter Kontrolle

Quelle: Freepik

Komplexität und mögliche Nachzahlungen

Lizenzmanagement ist eine funktionsübergreifende Aufgabe, die zunehmend an Komplexität gewinnt. Unternehmen riskieren hohe Nachzahlungen, wenn gegen Lizenzvereinbarungen verstoßen oder ein Software-Audit nicht bestanden wird. Zusätzlich erschweren ständige Änderungen der Lizenzmetriken und die wachsende Bedeutung des Cloud-Computings die Verwaltung von Softwarelizenzen. Es ist wichtig, Eigeninstallationen und mehrfach abonnierte Software im Blick zu behalten und ein funktionierendes Management in hybriden IT-Umgebungen sicherzustellen.

Effizientes Lizenzmanagement

Eine leistungsfähige Lizenzmanagement-Software muss verschiedene Anforderungen erfüllen, um den komplexen Herausforderungen gerecht zu werden. Die Software sollte alle gängigen Lizenzmodelle abbilden können, einschließlich Einzel-, Volumen- und Unternehmenslizenzen sowie User- und Clientlizenzierung. Dies umfasst auch CAL-Modelle und Serverlizenzierung. Eine präzise Lizenzzuordnung und ein hoher Automatisierungsgrad minimieren den manuellen Aufwand und gestalten die Verwaltung effizienter. Umfangreiche Risiko- und Einsparpotenzialanalysen helfen, Über- oder Unterlizenzierungen zu erkennen und schnell zu reagieren.

Zudem ist die präzise Zuordnung von Lizenzen zu verschiedenen Entitäten wie einzelnen Geräten, Benutzern oder Prozessoren eine entscheidende Funktion. Dies ermöglicht es Unternehmen, unabhängig davon, ob es sich um Vollversionen, Mietverlängerungen oder Wartungsvereinbarungen handelt, stets den Überblick über die Lizenzkosten zu behalten.

Integration und Compliance

Die Software sollte nahtlos in bestehende IT-Umgebungen integriert werden können, einschließlich der Anbindung an Active Directory und Cloud-Dienste. Zudem sollte die Software DSGVO-konform sein und durch eine unabhängige Prüfgesellschaften zertifiziert worden sein, um eine bestmögliche Vorbereitung für Audits sicherzustellen.

EFFIZIENTES LIZENZMANAGEMENT REDUZIERT KOSTEN UND ERHÖHT DIE IT-COMPLIANCE.

Julian Saalfrank, Lizenzmanagement-Experte, FCS Fair Computer Systems, www.fair-computer.de

Kostenreduktion durch Automatisierung

Der Einsatz einer effizienten Lizenzmanagement-Software, wie zum Beispiel Asset.Desk bringt zahlreiche Vorteile mit sich. Durch den hohen Automatisierungsgrad und die präzise Lizenzzuordnung können Unternehmen ihre Lizenzkosten erheblich senken. Unternehmen sind besser auf Software-Audits vorbereitet und können sicherstellen, dass sie stets konform mit den Lizenzvereinbarungen sind. Eine intuitive Benutzeroberfläche und Dashboards erleichtern die Verwaltung und das Monitoring von Lizenzen, selbst in großen und komplexen IT-Umgebungen. Die Implementierung der Software sollte schnell und unkompliziert umgesetzt werden können.

Modularer Ansatz

Während einige Unternehmen zusätzliche Funktionen benötigen, um ihre Prozesse zu optimieren, sind andere auf der Suche nach einer kosteneffizienten Lösung, die nur die notwendigsten Features bietet. Hier setzt ein modularer Ansatz an, der es Unternehmen ermöglicht, ihre Lizenzmanagement-Software nach Bedarf anzupassen.

Viele Lizenzmanagement-Softwares bieten neben den Grundfunktionen auch nützliche Zusatzfunktionen an. Unternehmen suchen oft nach Lösungen, die die manuelle Pflege und das Mapping automatisieren, um die Arbeitsbelastung signifikant zu reduzieren - hierfür sind beispielsweise Online Softwarekataloge verfügbar.

Durch das Application Metering können Unternehmen die Nutzungshäufigkeit und den letzten Einsatz von Softwareanwendungen verfolgen, was entscheidend für eine optimale Ressourcennutzung ist. Darüber hinaus ermöglichen Funktionen für Lizenzverträge, sämtliche Beschaffungsdetails, Laufzeiten und Verlängerungskonditionen der Lizenzen im Überblick zu behalten.

Optimierung der IT-Strategie

Effizientes Lizenzmanagement ist nicht nur ein optionales Extra, sondern ein wesentlicher Bestandteil der IT-Strategie eines jeden Unternehmens. Unternehmen sollten auf Lizenzmanagement-Software setzen, die durch umfangreiche Funktionen und einen hohen Automatisierungsgrad überzeugt. Eine gute Softwarelösung bietet transparente Lizenzverwaltung sowie umfangreiche Reporting- und Analysefunktionen. In einer dynamischen IT-Landschaft, in der sich Technologien und Lizenzmodelle ständig weiterentwickeln, ist effektives Lizenzmanagement unerlässlich. Unternehmen müssen ihre Lizenzierungsstrategien kontinuierlich überprüfen und anpassen, um rechtliche und finanzielle Risiken zu minimieren.

Zusammenfassend lässt sich festhalten, dass eine präzise Softwareinventarisierung, klare Lizenzbilanzen und die Abbildung aller gängigen Lizenzmodelle entscheidende Funktionen sind. Diese machen die Lösung zu einem unverzichtbaren Werkzeug für Unternehmen, um Compliance sicherzustellen und Kosten zu senken.

Julian Saalfrank

Automatisierung im SAP-Support

EFFIZIENTERE ABLÄUFE DURCH KÜNSTLICHE INTELLIGENZ

SAP-Anwendungen bilden in vielen Unternehmen geschäftskritische Prozesse ab. Der reibungslose Ablauf dieser Prozesse wird im operativen Betrieb durch den SAP-Support unterstützt, der bei technischen Problemen oder SAP-bezogenen Anfragen die erste Anlaufstelle für SAP-Anwender in Unternehmen ist.

Ein Großteil der eingehenden Anfragen betrifft die Benutzer- und Berechtigungsverwaltung, zum Beispiel das Zurücksetzen von Passwörtern, die Beantragung von Rollen oder die Diagnose und Behebung von Berechtigungsfehlern. Deren Bearbeitung erfordert aufwändige manuelle Prüfschritte durch SAP-Experten, die über genaue Kenntnisse der Benutzer-, Berechtigungs- und Rollenstruktur sowie der spezifischen SAP-Landschaft verfügen müssen.

Vor diesem Hintergrund wird die Bearbeitungszeit von SAP-Anfragen maßgeblich durch zwei Faktoren beeinträchtigt. Bis zu 70 Prozent der SAP-Tickets werden unvollständig oder fehlerhaft erstellt, was zusätzliche Rücksprache mit dem Anwender erfordert. Zudem sind die für die Bearbeitung erforderlichen SAP-Experten in der Regel bereits durch interne Großprojekte wie einer S/4-Transformation stark ausgelastet.

Praxisbeispiel SAP Servicedesk

Durch jüngste Fortschritte im Bereich der künstlichen Intelligenz, insbesondere im Bereich von generativer KI, rücken nun vor allem Chatbots zur Automatisierung von Supportaktivitäten in den Fokus von Unternehmen.

Am Beispiel des SAP-Servicedesks lässt sich das Potenzial des Einsatzes KI-gestützter Assistenten gut beleuchten. Voraussetzung ist die Integration des Chatbots in zentrale IT-Systeme des Unternehmens, wie die Einbindung des Chatbots in die Business-Kommunikationssoftware wie Microsoft Teams als auch die Anbindung an Backend-Systeme wie das ITSM-Tool und die SAP-Landschaft.

Der Anwender kann dann über die gewohnte Chat-Oberfläche seine Supportanfrage an den Chatbot richten. Dabei findet im Hintergrund eine Authentifizierung statt, die die Grundlage für eine automatisierte Ermittlung des SAP-Users liefert und eine individuelle Unterstützung durch den Chatbot ermöglicht.

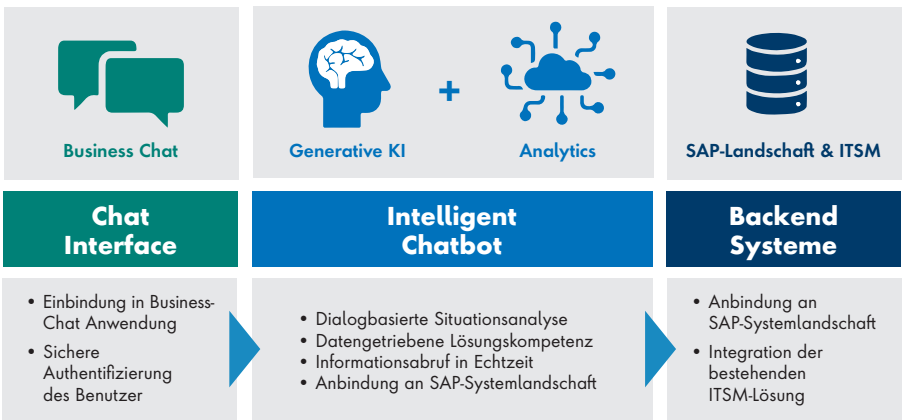
Alle Texteingaben des Anwenders werden mit Hilfe von Large Language Models klassifiziert und eingeordnet. Diese KI-Modelle eignen sich besonders gut für die Verarbeitung von Sprache und können zur Bestimmung der Problemkategorie, etwa Rollenbeantragung oder Berechtigungsproblem, genutzt werden. Auch wichtige Kontextinformationen werden aus der Eingabe extrahiert und bei fehlenden Informationen direkt beim Nutzer erfragt.

Durch die Anbindung an die SAP-Landschaft ist der Chatbot in der Lage, alle gesammelten Informationen in Echtzeit zu validieren und den Nutzer bei der Vervollständigung seiner Anfrage individuell zu unterstützen. Aufwändige manuelle Prüfschritte können so automatisiert werden. Die Daten fließen in eine automatisierte Problemdiagnose ein, die entweder sofort durch den Chatbot gelöst werden kann oder als Lösungsvorschlag im Ticket hinterlegt wird. Abschließend erfolgt die Erstellung des Tickets im ITSM-Tool. Dem Bearbeiter liegt dann ein validiertes Ticket mit allen notwendigen technischen Informationen inklusive Lösungsvorschlag vor.

Fazit

Der Einsatz KI-gestützter Chatbots kann mit dem dargestellten Ansatz die Bearbeitungszeit für bestimmte Ticketkategorien um bis zu 90 Prozent reduzieren. Gleichzeitig standardisiert der Ansatz Diagnose- und Lösungsprozesse, was nicht nur die Servicequalität erhöht, sondern auch die Security und Compliance innerhalb der SAP-Landschaft verbessert.

Dmitrij Spolwind
KPMG AG Wirtschaftsprüfungsgesellschaft
www.kpmg.com



Daten immer und überall schützen

SICHERHEITSRICHTLINIEN KONSEQUENT DURCHSETZEN

Die Zeiten, in denen Unternehmensdaten auf das Unternehmensnetzwerk beschränkt waren, sind längst vorbei. Heute befinden sie sich praktisch überall: im Web, in der Cloud und auf den verschiedensten Endgeräten – auch auf privaten. Wie lässt sich Datensicherheit in einer solchen Welt zuverlässig und effizient umsetzen?

Damit ein Unternehmen funktioniert, müssen Mitarbeiter unkompliziert auf alle Daten zugreifen können, die sie im Arbeitsalltag benötigen – jederzeit, von jedem Ort aus und mit dem Gerät ihrer Wahl. Dadurch entstehen unzählige Datenflüsse, die sich nur schwer kontrollieren lassen. Unternehmen verlieren zunehmend den Überblick, welche Daten sie überhaupt besitzen, wo diese gespeichert sind und wer auf sie zugreift. Dadurch fällt es ihnen schwer, die Datenflüsse über alle Kanäle hinweg zu überwachen und Sicherheitsrichtlinien konsequent durchzusetzen. Möglich ist das allerdings schon – die fünf wichtigsten Schritte für einen Ansatz, der überall Datensicherheit bietet:

#1 Zentrale Richtlinien für Cloud und Endgeräte definieren

#2 Web- und DLP-Richtlinien vereinheitlichen

#3 Daten in E-Mails schützen

#4 Angepasst und in Echtzeit auf Risiken reagieren

#5 Dark Data klassifizieren, bereinigen und schützen

www.forcepoint.com/de

Das Beste aus zwei Welten

NAHTLOSE INTEGRATION VON ERP UND CRM

ERP- und CRM-Lösungen gehören zu den wichtigsten Säulen innerhalb der Unternehmens-IT. Während im ERP-System die kaufmännischen Prozesse abgewickelt werden, dient eine CRM-Applikation Vertriebs- und Marketingabteilungen vor allem zur Kundenbetreuung und Planung von Marketingkampagnen. Die Verzahnung beider Systeme ist überaus sinnvoll.

Vorteile einer ERP-CRM-Integration

Eine Integration von ERP- und CRM-Lösungen ermöglicht vor allem eine nahtlose Synchronisation von Stamm- und Transaktionsdaten, sodass eine redundante Dateneingabe und -haltung entfällt. Die Mitarbeitenden gewinnen eine umfassende Sicht auf die Kunden des Unternehmens. Sie haben beispielsweise Zugriff auf die Bestellhistorie sowie die bevorzugten Produkte der Kunden und können so passgenaue Angebote unterbreiten oder ergänzende Lösungen vorschlagen. Zugleich überblicken sie die Produktionsauslastung und die Lagerbestände. Dies versetzt Mitarbeitende in die Lage, den Kunden konkrete Liefertermine zu nennen und Fragen zum Status einer Bestellung zu beantworten.

Neben der Reduzierung der manuellen Dateneingabe und der damit verbundenen Verringerung der Fehlerquote sowie einer besseren Customer Experience werden durch die Integration der beiden Lösungen auch Geschäftsprozesse optimiert. Alle Abteilungen nutzen dieselben Daten, was zu effizienten und koordinierten Abläufen führt. Werden überdies die umfassenden Daten des ERP-Systems den Analysetools von CRM-Systemen zur Verfügung gestellt, resultieren daraus aussagekräftige Berichte, die zu einer besseren Entscheidungsfindung beitragen.

Integrationsmöglichkeiten

Grundsätzlich gibt es zwei Möglichkeiten der Vernetzung: Unternehmen können entweder die einzelnen Systeme punktuell über APIs miteinander verbinden oder aber eine Integrationsplattform einführen.

Bei einer API-basierten Integration werden das ERP- und das CRM-System über deren Konnektoren direkt miteinander verbunden. Der Vorteil dieses Ansatzes ist, dass sich die Anbindung vergleichsweise schnell umsetzen lässt. Als Nachteil muss eine solche Point-to-Point-Anbindung bei jedem Releasewechsel neu erstellt werden und ist nicht skalierbar. Sollen weitere Systeme angedockt werden, sind zusätzliche Anbindungen zu programmieren. Dies führt neben hohen Kosten schließlich zu einer unübersichtlichen Integrationslandschaft mit einem immensen Wartungsbedarf.

Durch den Einsatz einer Integrationsplattform, auch Middleware genannt, lässt sich das Vorhaben mit deutlich weniger Programmierkenntnissen bewerkstelligen. Ein weiterer Vorteil ist die höhere Skalierbarkeit im Hinblick auf die Anbindung weiterer Anwendungen. Als nachteilig gilt für diesen Ansatz, dass die Einführung einer solchen Middleware mit einem höheren Aufwand verbunden ist. Natürlich müssen auch zusätzliche Lizenzkosten einkalkuliert werden. Zudem kann die Komplexität von Middleware-Lösungen das Hinzuziehen externer Integrationsarchitekten erforderlich machen, was zu Beginn weitere Kosten verursacht.

Zusammenfassend lässt sich sagen, dass eine API-basierte Integration eine taktische Entscheidung ist, die es Unternehmen ermöglicht, ERP- und CRM-Systeme kostengünstig und schnell miteinander zu verbinden. Die Einführung einer Middleware hingegen ist ein strategischer Entschluss, der sich mittel- bis langfristig auszahlt und insbesondere in einer IT-Landschaft mit zahlreichen Applikationen von Vorteil ist.

Erfolgsfaktoren der ERP-CRM-Integration

➤ **Prozesse betrachten und optimieren:** Im Rahmen eines Integrationsprojektes ist es empfehlenswert, zunächst die Prozesse zu betrachten, an denen ERP- oder CRM-Systeme beteiligt sind. Hier ist vor allem der Austausch zwischen der IT- und den Fachabteilungen gefragt. Aus den gewonnenen Erkenntnissen können die Anforderungen an die Integration exakt definiert werden. Dies erfordert eine sorgfältige Sondierung und Planung, die den reibungslosen Betrieb sowie die künftige Skalierbarkeit sicherstellt und gleichzeitig den sogenannten „IT Delivery Gap", also die Lücke zwischen den Anforderungen aus dem Business und deren Umsetzung durch die IT, nachhaltig schließt.

➤ **Daten konsolidieren:** Wenn Unternehmen ihre ERP- und CRM-Systeme bisher isoliert voneinander betrieben haben, dann liegen die Kundenstammdaten redundant vor. Die Wahrscheinlichkeit ist hoch, dass sie aufgrund unterschiedlicher Schreibweisen oder der variierenden Struktur inkonsistent sind. Die Bereinigung und Konsolidierung dieser Daten ist notwendig, um das künftige Master-Data-Management auf ein solides Fundament zu setzen. Der Markt bietet heute leistungsfähige Tools, die dabei helfen, redundante Daten aufzuspüren und zu konsolidieren, ebenso enthalten einige CRM-Systeme entsprechende Funktionen.

DIE VERBINDUNG VON ERP UND CRM SORGT FÜR BESSEREN KUNDENSERVICE, OPTIMIERTE PROZESSE UND SPÜRBARE EFFIZIENZSTEIGERUNG.

Abdelghani Faiz,
Geschäftsführer, Integration Matters GmbH,
www.integrationmatters.com

➤ **Sicherheitsaspekte beachten:** Vor allem der Einsatz von Cloud-Lösungen fordert Unternehmen, intensive Sicherheitsvorkehrungen zu treffen. Dazu sollten sie ein zentrales Governance-Modell etablieren, das Standards für die Anbindung von Softwarelösungen festlegt. Mit solchen Normen ist die Einhaltung definierter Sicherheitsstandards innerhalb einer digitalen Infrastruktur gewährleistet. Darüber hinaus helfen eine Multi-Faktor-Authentifizierung (MFA) und die Einrichtung von API-Gateways bei der Umsetzung einer strengen Zugriffskontrolle sowie mehrstufiger Schutzmaßnahmen. Nicht zuletzt sollten sensible Daten bei der Übertragung tokenisiert, also in einzelne Elemente zerlegt werden. Eine kontinuierliche Kontrolle, dass die Sicherheitsmaßnahmen zuverlässig funktionieren, ist unabdingbar.

➤ **Hohe Nutzerakzeptanz erreichen:** Die Erfahrung zeigt, dass der Erfolg von IT-Projekten zu etwa 80 Prozent von den involvierten Personen abhängt und nur zu rund 20 Prozent von der eingesetzten Technik. Daher ist es erforderlich, alle Stakeholder von Anfang an in das Projekt einzubeziehen und die Kommunikation verständlich auszulegen. Fragestellungen wie jene, was bis wann erreicht werden soll und warum oder wie Abteilungen davon profitieren können, sollten eindeutig beantwortet werden. Ebenso empfiehlt sich ein Skizzieren des anstehenden Veränderungsprozesses sowie die Erläuterung, welche Meilensteine damit verbunden sind und was das für die betroffenen Mitarbeitenden bedeutet. Während des Projekts sollten regelmäßige Meetings stattfinden, in denen die IT-Verantwortlichen über die Projektfortschritte informieren und zugleich die Ideen und Einschätzungen der Anwender einholen.

Fazit

Die Integration von ERP- und CRM-Systemen bietet Unternehmen zahlreiche Vorteile. Dazu gehören eine höhere Datengenauigkeit, effizientere Prozesse und eine umfassende Sicht auf die Kunden. Gelingen kann diese Verbindung „zweier Welten" mit einer klaren Planung, der Nutzung bewährter Methoden und der Wahl geeigneter Technologien.

Abdelghani Faiz

ERP-as-a-Service

WIE DER MITTELSTAND SICH SEINER KETTEN ENTLEDIGT

Der deutsche Mittelstand, das Rückgrat der Wirtschaft, durchlebt aktuell schwierige Zeiten. Im Wettrennen um eine Vorreiterrolle in Sachen Technologie und Innovationskraft tritt Deutschland auf der Stelle – als würde es von Ketten zurückgehalten. Sind diese jedoch rein symbolischer Natur. Die gegenwärtige Lage lässt sich durchaus als bescheiden titulieren. Die aktuelle Konjunkturprognose des Ifo Instituts erwartet für das laufende Jahr ein Wirtschaftswachstum um 0,2 Prozentpunkte. Auch die Innovationsfähigkeit bleibt hierzulande immer wieder auf der Strecke. Der letztjährige Innovationsindikator des Bundesverbands der Deutschen Industrie (BDI) sieht Deutschland konstant im Mittelmaß versinken – die Spitzenreiter aus der Schweiz, Singapur und Dänemark eigentlich nur noch mit dem Fernglas erkennbar. Das lahme Tempo hat diverse Ursachen. Die Personaldecke ist ob des Fachkräftemangels dünn, und die vorhandene Belegschaft gekettet an Tätigkeiten, die der Wertschöpfung nicht helfen.

Es stellt keine gewagte These auf, wer behauptet, dass es in der Vergangenheit bereits leichtere Zeiten für die deutsche Wirtschaft gegeben hat. Die Weltlage, deren Bezeichnung als angespannt wohl eine maßlose Untertreibung darstellen dürfte, nimmt Einfluss auf nahezu alle Geschäftsfelder. Die Gegebenheiten am globalisierten Markt unterliegen ständigen Veränderungen, die entsprechende Anpassungen von Seiten der Unternehmen verlangen. Hohe Kosten für Ressourcen wie Energie, Rohstoffe und Personal müssen gesenkt werden, während die zum Teil komplexen Geschäftsprozesse diese erbarmungslos binden. Konstante Ressourcenengpässe halten den Mittelstand an Ort und Stelle – die Ketten anliegend.

Effizienz als Schlüssel in die Freiheit

Einen großen Schritt auf dem Weg, die metaphorischen Fesseln zu lösen, stellt die Wahl des passenden ERP-Systems (Enterprise Resource Planning) dar. Unterschieden wird grundsätzlich zwischen On-Premises und ERP-as-a-Service (ERPaaS). Während die erstgenannte Variante sämtliche Prozesse im Unternehmen hält, kommt es bei ERP-as-a-Service zu deren vollumfänglicher Auslagerung in eine Cloud. Noch setzt die Mehrzahl der KMU in Deutschland auf On-Premises, doch der Umsatz, der durch cloud-basierte ERP-Lösungen erzielt wird, steigt kontinuierlich. ERPaaS erweist sich gegenüber seinen konservativen Pendants immer häufiger als die im Umgang mit den zur Verfügung stehenden Ressourcen effizientere Herangehensweise.

On-Premises erfordert einen immensen personellen Aufwand für die Wartung und Aktualisierung des Systems. Anpassungen an den Markt gehen so stets mit hohen Kosten einher und können ob der Frequenz ihrer derzeitigen Notwendigkeit sowie des dramatisch anmutenden Ausmaßes des Fachkräftemangels in der IT-Branche kaum in den gegebenen zeitlichen Abständen vorgenommen werden.

ERPaaS punktet währenddessen mit einer besonders kostengünstigen und schnellen Implementierung. Anpassungen in Form von Softwareupdates werden automatisch durch den Anbieter durchgeführt. Betriebe, die sich in der Wachstumsphase befinden oder mit saisonalen Schwankun-

ERPAAS LÄSST SICH SOWOHL FÜR DIE EVALUATION INTERNER GESCHÄFTSPROZESSE ALS AUCH FÜR DIE ANALYSE DER GEGENWÄRTIGEN SITUATION AM MARKT EINSETZEN.

Ertan Özdil,
Gründer und CEO, weclapp SE,
www.weclapp.com

gen konfrontiert werden, schätzen zudem die hohe Skalierbarkeit der cloud-gestützten ERP-Lösungen. Sie erlauben, die Ressourcennutzung je nach Bedarf zu senken oder zu erhöhen.

Mit ERP-as-a-Service zurück ins Spiel

ERPaaS trägt spürbar zur Komplexitätsreduzierung und Professionalisierung diverser Arbeitsabläufe bei. Durch die Implementierung von ERPaaS können viele Routineaufgaben aus verschiedensten Bereichen automatisiert werden. In der Finanzbuchhaltung kann die Berichterstattung automatisiert ablaufen, im Personalmanagement Gehaltsabrechnungen, Urlaubsplanung und Zeiterfassung ohne den Einsatz personeller Ressourcen erfolgen. Die Anwendungsbereiche von ERPaaS-Lösungen umfassen darüber hinaus unter anderem auch das Produkt- und Projektmanagement, die Lagerverwaltung oder den Vertrieb. Die Folge ist eine signifikante Reduktion des erforderlichen manuellen Aufwands auf nahezu allen Ebenen, die wiederum für eine Senkung der Fehleranfälligkeit verantwortlich zeichnet.

Die freigewordenen personellen Kapazitäten können nun für strategisch wichtigere Aufgaben genutzt, Effizienz und Produktivität gesteigert werden. ERPaaS lässt sich sowohl für die Evaluation interner Geschäftsprozesse als auch für die Analyse der gegenwärtigen Situation am Markt einsetzen. KMU können auf diese Weise die eigenen Geschäftsprozesse effizienter gestalten. Extern helfen die Anwendungen, die für eine gute Wettbewerbsfähigkeit elementaren Anpassungen an den Markt frühzeitig zu vollziehen. ERPaaS lassen mittels Datenanalyse in Echtzeit aktuelle Entwicklungen innerhalb einer Branche erkennen, evaluieren die Bedürfnisse der Klientel und helfen so, die strategische Entscheidungsfindung massiv zu beschleunigen. Unternehmen, welche die Vorteile von ERPaaS erkennen, können sich gegenüber ihren Mitbewerbern entscheidende Wettbewerbsvorteile am Markt verschaffen – und sind nicht nur sprichwörtlich Back in Business.

Raum für Innovation entsteht

Die erhebliche Steigerung der betrieblichen Effizienz verschafft dem Mittelstand die Freiheit, Ressourcen, die nun nicht länger in der Ausübung von Routinetätigkeiten gefragt sind, der Förderung von Innovation zukommen zu lassen. Es eröffnen sich an diesem Punkt vielfältige Möglichkeiten, Innovationen voranzutreiben. Möglich sind Investitionen in die Forschung und die Entwicklung neuer Produkte und Technologien. Die Weiterbildung und Schulung der vorhandenen Belegschaft ist nicht minder lohnend. Die Mitarbeitenden verbessern ihre Fähigkeiten sowie ihr Wissen und fördern so selbst eine Kultur der kontinuierlichen Verbesserung und Innovation. Auch die Erschließung neuer Geschäftsfelder oder die Implementierung fortschrittlicher Technologien sind als Konsequenz des Einsatzes von ERPaaS im Bereich des Möglichen. Dieser Text soll keineswegs den Anschein erwecken, dass durch einen kollektiven Umstieg auf ERP-as-a-Service sämtliche Probleme des deutschen Mittelstandes gelöst würden, doch versetzt ERPaaS ihn in die Lage, sich zumindest der schwersten seiner Ketten zu entledigen.

Ertan Özdil

Nachhaltige Produktion

WENN ÖKOLOGIE UND WIRTSCHAFTLICHKEIT HAND IN HAND GEHEN

Nachhaltiges Handeln mit dem Ziel einer klimaneutralen Produktion rückt auch im Umfeld der Losgröße 1+ in den Fokus. Verschiedenste ökonomische, ökologische, politische und gesellschaftliche Faktoren wirken auf die Entscheidungsträger in mittelständischen Fertigungsunternehmen ein. Um Regularien zu erfüllen und Erwartungen zu entsprechen, benötigen sie nachvollziehbare Strategien für ein wirksames Klimamanagement.

Für eine schnelle Umsetzung ist dabei ein schrittweises Vorgehen vorteilhaft, das sich an gesetzlichen Vorgaben und realistischer Umsetzbarkeit orientiert. Ein Aspekt ist, dass nachhaltiges Produzieren dank innovativer Verfahren die Profitabilität steigern kann.

Auch die Verantwortlichen in mittelständischen Unternehmen sind gefordert, sich mit Themen wie der EU-Richtlinie zur Nachhaltigkeitsberichterstattung von Unternehmen (Corporate Sustainability Reporting Directive, kurz CSRD) oder dem Digitalen Produktpass (DPP) zur datentechnischen Erfassung des vollständigen Lebenszyklus' aller in ihren Produkten verbauten Bauteile und Materialien intensiv zu befassen.

Selbst, wenn für kleinere Betriebe mit weniger als 250 Mitarbeitenden im Rahmen gewisser Übergangszeiten noch nicht alle Regularien gelten, die größere Unternehmen und Konzerne erfüllen müssen, ist es ratsam, das Thema weit oben auf die Tagesordnung zu setzen. Denn im Zuge eines generell gestiegenen Umweltbewusstseins schauen beim Thema Nachhaltigkeit alle Marktbeteiligten genauer hin.

Die Kategorisierung der Treibhausgasemissionen

Gemäß dem Greenhouse Gas Protocol unterteilt sich der CO_2-Fußabdruck von Firmen in drei Kategorien, die sogenannten Scopes. Scope 1 umfasst alle direkten und eigenerzeugten Treibhausgasemissionen, die vorrangig aus der Verbrennung von Primärenergieträgern wie Heizöl, Erdgas, Benzin oder Diesel entstehen. Scope 2 umfasst die energiebezogenen indirekten Treibhausgasemissionen, zu denen verbrauchte Sekundärenergieträger wie Strom, Fernwärme,

Dampf oder Kühlungsenergie zählen. Scope 3 schließlich umfasst alle sonstigen indirekten Treibhausgasemissionen, die sich schwerpunktmäßig aus den Unternehmenstätigkeiten und den gesamtbetrieblichen Abläufen ergeben.

Die Emissionen dieser dritten Gruppe entstammen diversen Quellen entlang der Wertschöpfungskette, die nur zum Teil unter der Kontrolle der produzierenden Unternehmen stehen, wodurch sie wesentlich schwerer zu identifizieren und damit auch wesentlich schwerer zu reduzieren sind. Dazu zählen Aspekte des Transportwesens und der Supply Chain ebenso wie der Bezug und die Nutzung von Waren und Dienstleistungen, die Nutzung von Papier und Wasser, die Entsorgung von Abwasser und Müll, der Energieverbrauch in vermieteten oder angemieteten Immobilien und Sachanlagen oder auch Geschäftsreisen.

Ein weiterer Punkt ist die Berücksichtigung des kompletten Lebenszyklus' der produzierten Produkte mitsamt der von ihnen verbrauchten Ressourcen und Materialien sowie ihrer Entsorgung. Um die Anteile der Treibhausgasemissionen der einzelnen Scopes in Relation zueinander zu setzen, sei auf das Ergebnis einer Studie des Carbon Disclosure Project (CDP) von 2022 verwiesen. Darin heißt es, dass bei jenen Unternehmen, deren Zahlen dem CDP vorliegen, die Emissionen aus der Lieferkette durchschnittlich elfmal so hoch sind wie die betrieblichen, unmittelbar die Fertigung betreffenden Ausstöße.

Schrittweises Vorgehen

Welche konkreten Schritte sollten Mittelständler nun aus dem Umfeld der Losgröße 1+ auf dem Weg zu mehr Klimaneutralität in welcher Reihenfolge einleiten? Zunächst empfiehlt es sich, eine oder mehrere Personen zu benennen, die für die Bearbeitung von Nachhaltigkeitsthemen zuständig sind und die Relevanz des Themas gemeinsam mit der Geschäftsführung in das jeweilige Unternehmen tragen.

Nachdem vorab der aktuelle Treibhausgasausstoß ermittelt wurde, geht es im Anschluss um die Formulierung realistischer Klimaschutzziele für den eigenen Betrieb. Zuerst sollte es dann um die Senkung der bislang erzeugten Emissionen durch geeignete Energieeffizienzmaßnahmen und danach um die Gewinnung und die Nutzung erneuerbarer Energien gehen. Wo sich der Energieverbrauch als Folge der Produktfertigung nicht vermeiden lässt, rücken kompensatorische Maßnahmen für den erfolgten ökologischen Schaden in den Fokus. Bestes Beispiel hierfür ist der EU-Emissionshandel für CO_2.

Wichtig ist es, die eingeleiteten Maßnahmen zu dokumentieren und – wo immer es möglich und sinnvoll ist – von seriösen Institutionen zertifizieren zu lassen, bevor sie an alle Marktteilnehmer kommuniziert werden. Ebenfalls essenziell ist die immer wiederkehrende Bewertung und Überprüfung der eigenen Aktivitäten, um weiteres Verbesserungspotenzial zu heben.

Schaut man sich in der Praxis um, zeigt sich schnell, dass nachhaltiges Handeln nicht nur ökologisch sinnvoll ist, sondern auch auf anderen Ebenen Vorteile bringt.

Der bayerische Verpackungsmaschinenhersteller Somic setzt auf „gelebte Regionalität", was unter anderem bedeutet, dass die meisten Zulieferer im direkten Umkreis des Firmenstandorts angesiedelt sind. Die kurzen Transportwege und der Einsatz nachhaltiger Transportlösungen minimieren dabei nicht nur den eigenen ökologischen Fußabdruck, sondern sorgen darüber hinaus auch für eine schnelle und sichere Versorgung mit den notwendigen Teilen.

Nachhaltigkeit in der Praxis

Ein weiterer Baustein im Nachhaltigkeitskonzept des Unternehmens ist eine möglichst lange Lebensdauer der Maschinen. So wird eine spätere Anpassung auf neue Produkte oder Formate von Beginn an eingeplant. Die Programmierung neuer Formatprogramme mittels Remote-Control geht nicht nur schnell vonstatten, son-

dern spart zudem Reisekosten und viele Auto- oder Flugkilometer. Außerdem können neue Formatteile auch für alte Maschinen gefertigt werden. Der Einsatz modernster, servogesteuerter Antriebe reduziert darüber hinaus den Stromverbrauch, etwa durch Energierückgewinnung.

Ähnlich wie Somic setzt auch der Siegerländer Walzanlagenhersteller Achenbach Buschhütten auf technologische Innovation zur Erlangung von größerer Klimaneutralität. Dort verpflichtet man sich getreu dem Leitbild Green.Lean.Digital. nicht nur, die eigene Produktion und das Verhalten im Arbeitsalltag nachhaltig zu gestalten, sondern möchte letztlich durch die Produkte selbst langfristig den größten Einfluss in Sachen Klimaneutralität nehmen. Nämlich dann, wenn die Kunden dank innovativer Produktlösungen und nachhaltiger Produktionsverfahren weniger Energie und/oder weniger Verbrauchsmittel benötigen. Ein Beispiel sind die modernen Rektifikationsanlagen, welche die thermische Abscheidung von Fremdölen aus dem Walzöl und dessen Rückführung in neuwertiger Qualität in den Produktionskreislauf übernehmen.

Technologische Innovation senkt Verbrauch

Im thermischen Bereich bietet Achenbach innovative Systeme an, darunter eines zur Bandkanteninduktion, das Energie zielgenau an den Bedarfspunkt leitet. Dies führt zu einer drastischen Einsparung und höheren Ressourceneffizienz durch weniger Bandabrisse. Auch im Bereich der Antriebssysteme für Walzwerke hat das Unternehmen ein neues, energieeffizientes Produkt entwickelt, das auf verlustbehaftete Komponenten verzichtet. Dank einem Energy Management Tool können Walzanlagenbetreiber den Gesamtstromverbrauch und den Verbrauch einzelner Antriebe überwachen und in Echtzeit zu Produktionsdaten setzen, um Einsparpotenziale zu finden. Auf dieser Basis lässt sich auch der produktbezogene CO_2-Fußabdruck verfolgen. So bietet der Hersteller die Möglichkeit, perspektivisch das umzusetzen, was dem Unternehmen selbst gelungen ist: eine Reduzierung des CO_2-Ausstoßes von 60 Prozent zwischen 2013 und 2023. Das Ziel besteht darin, bis 2030 am Standort bei „Net Zero“ zu sein.

WIE UNTERSTÜTZT ERP DIE NACHHALTIGKEITSBESTREBUNGEN?

Um perspektivisch schonender mit Ressourcen umzugehen, sind Unternehmen künftig verpflichtet, ihre Verbräuche im Rahmen des CSR-Nachhaltigkeitsberichts zu erfassen und zu dokumentieren. Die dadurch angestrebte Senkung der Materialverbräuche und CO_2-Emissionen liegt auch im Interesse der Firmen selbst. Denn auf diese Weise können sie weiterhin wettbewerbsfähige Preise bieten.

Bei der Reduzierung des Material- und Energiebedarfs spielt das ERP-System eine entscheidende Rolle. Als unternehmensweite Datendrehscheibe ist es eines seiner prädestinierten Einsatzgebiete, die gesamten logistischen Prozesse des Warentransports im Einkauf, im Versand oder bei Fremdvergaben zu erfassen und ressourcenschonend zu steuern.

Fazit

Sowohl Somic als auch Achenbach zeigen, was technologisch führende Mittelständler aus dem Umfeld der Losgröße 1+ leisten können, um nicht nur selbst ressourcen- und klimaschonender zu produzieren, sondern dies auch ihren Kunden zu ermöglichen. Wenn eine ökologischere Herstellung von Produkten gleichzeitig die Wirtschaftlichkeit unterstützt, profitieren alle: Umwelt, Gesellschaft und Unternehmen.

Guido Piech | www.ams-erp.com

IT UND DIGITALES FÜR AUFSICHTSRÄTE UND BEIRÄTE

WAS SIE ALS AUFSICHTSRAT ODER BEIRAT ÜBER IT UND DIGITALES WISSEN SOLLTEN

IT und Digitales für Aufsichtsräte und Beiräte; Daniela Hellwig, Karl-Heinz Schulte, DC Pubslishing; 04-2024

„Die Digitalisierung und damit die Informationstechnologie wird immer stärker zu einem Schlüsselfaktor für den Erfolg von Unternehmen", sagt Karl-Heinz Schulte, Interim CIO und Digitalbeirat mit Schwerpunkt auf digitale Transformationen und Umbrüche. „Nur wenn es gelingt, Geschäftsstrategie und IT in Einklang zu bringen, können sich Unternehmen heute und vor allem in Zukunft überhaupt noch erfolgreich am Markt behaupten", ergänzt Daniela Hellwig, Expertin für Transformation und Kommunikation. Jetzt haben die beiden zusammen ein Buch geschrieben: „IT und Digitales für Aufsichtsräte und Beiräte".

Auf 256 Seiten arbeiten die Autoren alle Themenbereiche ab, bei denen ein Aufsichtsrat oder Beirat ein Grundgerüst an Expertise aufweisen sollte: Business IT Fit, das Haus der IT, IT Target Operation Model, IT-Sourcing, Governance und IT-Management, IT-Frameworks, IT-Risikomanagement, IT-Security, Notfallplanung, Backups und mehr. Ein Schwerpunkt wird auf das Thema Cybersecurity gelegt. Bei allen Aspekten machen die beiden Autoren klar, welche Verantwortung die oberste Unternehmensführung dabei trägt – und welche damit auch der Aufsichtsrat und Beirat als Beratungs- und Kontrollinstanz für Vorstand oder Geschäftsführung.

Das jüngste Werk aus der Serie „Praxiswissen für Aufsichtsräte und Beiräte" ist ein offizielles Lehrbuch der Steinbeis Augsburg Business School für die Kursreihe „Zertifizierter Aufsichtsrat und Beirat (m/w/d)". Das Buch erscheint im Verlag der Denkfabrik Diplomatic Council mit UN-Beraterstatus.

Transformation versus Change

UNTERSCHIEDE UND HERAUSFORDERUNGEN FÜR DIE NEUAUSRICHTUNG

Der Begriff Transformation ist zurzeit in aller Munde – ebenso der Begriff Zeitenwende. Doch was bedeutet er im Unternehmenskontext überhaupt? Das ist oft unklar! Ebenso, was einen Transformations- von einem Changeprozess unterscheidet.

Im Managementbereich hat sich nach dem Begriff Change ein neues Buzzword etabliert: Transformation. Noch vor wenigen Jahren wurde dieser Begriff eher selten in den Verlautbarungen der Unternehmen verwendet; heute hingegen findet man ihn im Zuge der digitalen Transformation der Wirtschaft und rasant fortschreitenden Entwicklung im Bereich der Künstlichen Intelligenz (KI) sowie der fundamentalen gesellschaftlichen Veränderungen, die sich im Umfeld der Unternehmen vollziehen, in fast allen Statements der Unternehmen, die deren Zukunft betreffen.

Nicht jeder Change ist eine Transformation

Im Gespräch mit firmeninternen Transformationsexperten und ihren externen Beratern stellt man jedoch oft fest: Den meisten fällt es schwer, genau zu sagen, was einen Transformations- von einem Change-Prozess und einen Transformations- von einem Change-Manager unterscheidet. Häufig werden die beiden Begriffe Transformation und Change synonym verwendet. Dabei gibt es zwischen ihnen durchaus Unterschiede.

Das Wort Change bezeichnet schlicht eine Veränderung und kann sich auf sehr viele Objekte und Prozesse beziehen. So ist es zum Beispiel auch ein Change- oder Veränderungsprozess, wenn in einem Unternehmen die PCs ausgetauscht oder die Wände neu gestrichen werden. Ein Change ist es auch, wenn Abläufe optimiert, Teams neuformiert oder Mitarbeiter eingestellt oder entlassen werden. Ein Change kann sich also, er muss sich aber nicht auf alle drei Ebenen beziehen, die zum Beispiel dem Beratungsdreieck von K&P zugrunde liegen, nämlich die Unternehmensstrategie, -kultur und -struktur (Prozesse, Abläufe).

Ein Change muss zudem nicht, er kann aber auch eine Einstellungs- und Verhaltensänderung der Mitarbeiter erfordern, denn bei ihm wird nicht notwendigerweise ein sogenannter „Musterwechsel" vollzogen. So ist es zum Beispiel auch ein Change, jedoch kein „Musterwechsel", wenn in einem Werk eines Autoherstellers die Mitarbeiter fortan Limousinen statt Geländewagen produzieren. Denn dann müssen sie zwar vermutlich einige Handgriffe neu lernen, sie müssen aber ihre Einstellung und ihr Verhalten nicht grundsätzlich ändern. Anders sieht dies hingegen schon aus, wenn ein Autohersteller beschließt: „Wir produzieren künftig statt Autos mit Verbrennungsmotoren nur noch E-Autos". Oder gar: „Wir entwickeln uns zu einem Mobilitätsanbieter." Denn dann ändern sich nicht nur die Produktions- und Leistungserbringungsprozesse, sondern das gesamte Unternehmen muss ein neues Selbstverständnis beziehungsweise eine neue Identität entwickeln, was auch neue Kompetenzen sowie Denk- und Handlungsmuster bei den Prozessbeteiligten erfordert.

Sich transformieren heißt sich neu erfinden

Generell versteht man unter einer Transformation den Prozess der gezielten Umgestaltung der „genetischen" Grundstruktur eines Systems – unabhängig davon, ob es sich hierbei zum Beispiel um eine Gesellschaft, ein Unternehmen oder einen Unternehmensbereich handelt. Im Verlauf dieses Prozesses

- definiert zum Beispiel ein Unternehmen sich selbst und einen großen Teil seiner Beziehungen zu seiner Umwelt neu und
- hinterfragt neben seiner Strategie und seinem Geschäftsmodell auch seine Geschäftsprozesse und gestaltet diese bei Bedarf radikal um.

Das Unternehmen (oder der Unternehmensbereich) erfindet sich sozusagen neu, um mittel- und langfristig seinen Erfolg zu sichern.

Vor dieser Herausforderung stehen zurzeit viele Unternehmen, denn unter anderem aufgrund solcher Ereignisse oder Phänomene wie:

- dem Ukraine-Krieg und Gaza-Konflikt,
- dem Entstehen einer multipolaren Weltordnung,
- den immer stärker spürbar werdenden Folgen des demografischen Wandels und Klimawandels sowie
- der rasant fortschreitenden technologischen Entwicklung nicht nur im Bereich der Künstlichen Intelligenz,

CHANGE-MANAGEMENT: DAS BERATUNGSDREIECK

(Quelle: Kraus & Partner)

ändern sich die Rahmenbedingungen des wirtschaftlichen und unternehmerischen Handelns aktuell fundamental - und sie werden sich weiter verändern. Oder anders formuliert: Nicht nur unsere Gesellschaft befindet sich aktuell in einer Zeitenwende, auch viele Unternehmen sehen sich mit einer solchen konfrontiert.

Ein solch fundamentaler Wandel tangiert alle drei der vorgenannten Ebenen von Unternehmen: ihre Strategie, ihre Kultur und ihre Struktur. Und ihre Mitarbeiter? Sie müssen sich und ihr Verhalten neu definieren und eine neue Identität zumindest bezogen auf ihre Funktion in der Organisation entwickeln.

Die Transformation eines Unternehmens lässt sich am ehesten mit der Metamorphose vergleichen, die viele Insekten im Laufe ihres Lebenszyklus durchlaufen. So gibt es zum Beispiel bei einem Schmetterling die Entwicklungsphasen Ei, Raupe, Puppe und Falter. Und beim Übergang von einem Entwicklungsstadium ins nächste wandelt sich das genetische Material vollständig um. Doch nicht nur dies! Eine Schmetterlingsraupe hat auch andere Fähigkeiten als der Falter am Ende des Entwicklungszyklus: Eine Raupe kann zum Beispiel nicht fliegen.

Das Unternehmen entwickelt eine neue Identität

Ähnlich verhält es sich bei der Transformation eines Unternehmens. Auch in diesem Prozess wird unter Rückgriff auf die vorhandenen Ressourcen wie zum Beispiel Erfahrungen oder Kompetenzen das System Unternehmen so radikal umgestaltet, dass die transformierte Organisation für Personen, die mit ihr längere Zeit keinen Kontakt hatten, kaum wiedererkennbar ist, weil neben ihrer Strategie, sich auch ihre Kultur und Struktur gewandelt haben. Das heißt, nach dem Durchlaufen eines Transformationsprozesses verfügt eine Organisation nicht nur über ein neues Selbstverständnis und eine neue Identität, sondern auch über neue Kompetenzen, weshalb auch ihre Mitarbeiter teils neue Fähigkeiten und Fertigkeiten brauchen.

So weit so gut! Es gibt jedoch auch Unterschiede zwischen der Metamorphose eines Schmetterlings und der Transformation eines Unternehmens. Bei einem Schmetterling ist der Transformationsprozess genetisch festgelegt: Erst Ei, dann Raupe, dann Puppe, dann Falter. Er läuft sozusagen automatisch ab. Bei der Transformation eines Unternehmens ist dies nicht der Fall. Hier gilt es vielmehr ausgehend von einer Vision durch sorgsam geplante Interventionen das System Unternehmen Schritt für Schritt gezielt zu entwickeln beziehungsweise zu verändern.

LETZTLICH IST JEDER TRANSFORMATIONSPROZESS EIN KOMPLEXER, MULTIDIMENSIONALER CHANGEPROZESS, DER SEINERSEITS WIEDER AUS EINER VIELZAHL VON CHANGEPROJEKTEN BESTEHT, DIE SICH WECHSELSEITIG BEEINFLUSSEN.

Prof. Dr. Georg Kraus, Inhaber, Kraus & Partner, www.kraus-und-partner.de

Transformationsprozesse sind komplexe Changeprozesse

Das heißt, letztlich ist jeder Transformationsprozess ein komplexer, multidimensionaler Changeprozess, der seinerseits wieder aus einer Vielzahl von Changeprojekten besteht, die sich wechselseitig beeinflussen. Entsprechend groß muss die Change-Management-Kompetenz der Personen sein, die die Verantwortung für den Transformationsprozess tragen. Sie müssen bei ihrer Arbeit zudem, um zwei Termini aus dem agilen Projektmanagement zu gebrauchen, inkrementell und iterativ vorgehen. Das heißt, sie müssen im Prozessverlauf immer wieder checken,

#1 erzielen wir mit unseren Veränderungsinitiativen die gewünschten Wirkungen und

#2 bewegen wir uns als Organisation in Richtung des angestrebten Ziels?

Ebenfalls muss bei Bedarf eine Kurskorrektur oder Änderung am Design des Gesamtprojekts vorgenommen werden. Entsprechend groß sollte neben ihrer analytischen, auch ihre kommunikative Kompetenz sein, um den Betroffenen oder Beteiligten die Notwendigkeit von Kurskorrekturen zu vermitteln.

Bei Transformationsprozessen ist das Ziel oft unklar

Komplex ist die Aufgabe, Transformationsprojekte zu planen und zu steuern, jedoch nicht nur aufgrund der vielen Einflussfaktoren und Wechselwirkungen, die es hierbei zu berücksichtigen gilt.

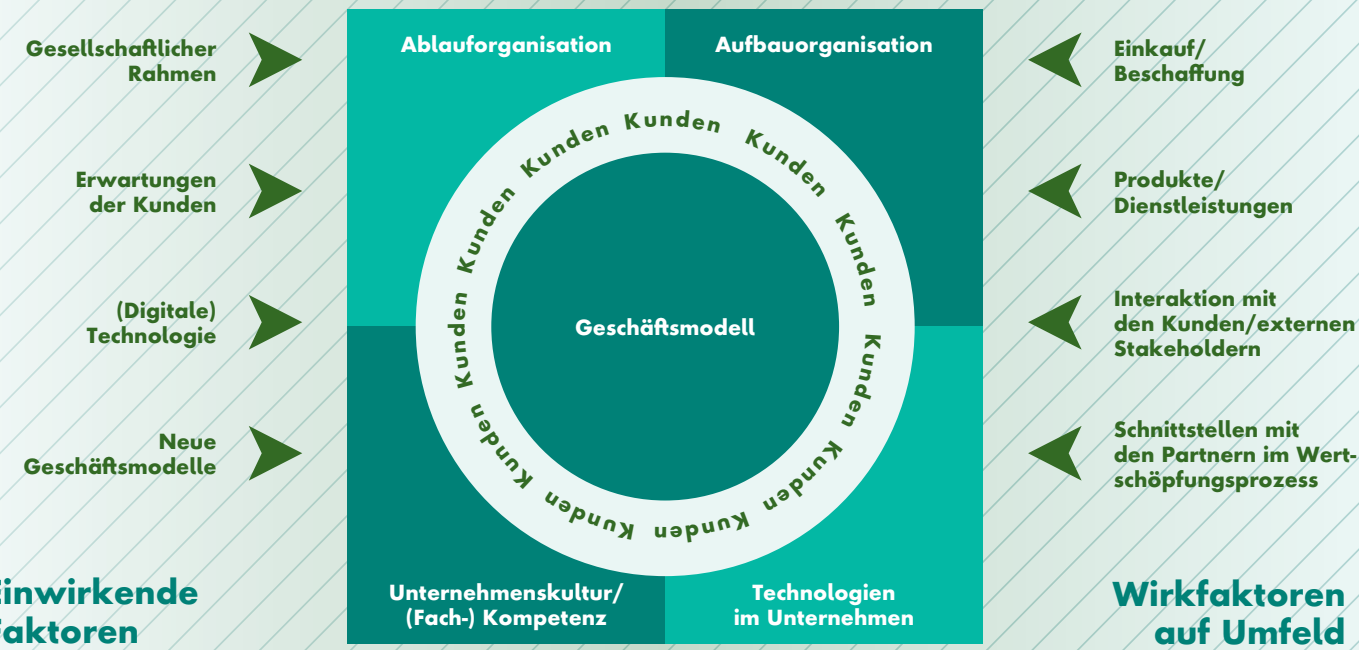
Hinzu kommt, bei der Metamorphose eines Schmetterlings steht neben dem Ablauf auch das Endergebnis des Transformationsprozesses zu dessen Beginn bereits fest: Aus der verpuppten Raupe wird, sofern sie zwischenzeitlich kein Vogel frisst, ein Falter, der nach wenigen Tagen stirbt.

Anders ist dies bei der Transformation von Unternehmen. Hierbei steht in der

TRANSFORMATION VON UNTERNEHMEN

Einwirkende Faktoren und Wirkfaktoren auf Umfeld

(Quelle: Dr. Kraus & Partner)



Regel auch die Vision, also das angestrebte Endziel der angestrebten Transformation unter Vorbehalt – unter anderem, weil dieser Prozess, der sich oft über mehrere Jahre erstreckt, sich in einem dynamischen Umfeld vollzieht. So kann heute zum Beispiel noch kein Top-Manager in der Automobil-Industrie mit Gewissheit sagen:

- Wie werden in 15 oder 20 Jahren die Autos beziehungsweise menschlichen Fortbewegungsmittel konstruiert und gebaut sein?
- Wer sind dann, sofern wir noch existieren, unsere schärfsten Mitbewerber? Und:
- Wird es dann überhaupt noch einen motorisierten Individualverkehr geben oder ist dieser dann im Gefolge des Klimawandels zumindest in den Ballungsräumen verboten?

Die Manager in der Automobil-Industrie können sich beim Entwickeln der Vision für ihr Unternehmen also bestenfalls von begründeten Vermutungen, die auf gewissen Trends und Entwicklungslinien sowie Daten und Annahmen basieren, leiten lassen. Wie sich der Markt ihres Unternehmens und dessen Umfeld in 10, 15 oder gar 20 Jahren tatsächlich gestalten wird, wissen sie jedoch noch nicht. Trotzdem müssen die Top-Manager heute bereits damit beginnen, ihr Unternehmen zukunftsfit zu machen. Entsprechendes gilt für das Management der Unternehmen in nahezu allen Branchen.

Transformationsprozesse erfordern eine hohe Agilität

Deshalb haben die Transformationsverantwortlichen gar keine andere Wahl, als bei der Projektplanung und -steuerung agil zu sein und zu bleiben, selbst wenn die im Rahmen des Gesamtprojekts stattfindenden Teilprojekte dann klassisch oder hybrid gemanagt werden. Entsprechend groß sollte neben ihrer Change- auch ihre Projekt-Management-Kompetenz sein. Zudem sollten sie reife Führungspersönlichkeiten mit einem starken Standing in ihrer Organisation sein, denen die Beteiligten, wenn nicht gerne, so doch bereitwillig folgen – unter anderem, weil sie ihnen nicht nur aufgrund ihrer fachlichen Kompetenz, sondern auch Persönlichkeit vertrauen.

Prof. Dr. Georg Kraus

it management

AUSGABE 09-10/2024
ERSCHEINT
AM 3. SEPTEMBER 2024

UNSERE THEMEN

DSAG-Spezial
Cloud & Edge Computing
Digitalisierung

it security

AUSGABE 09-10/2024
ERSCHEINT
AM 3. SEPTEMBER 2024

UNSERE THEMEN

Digitale Identitäten
it-sa Spezial
Threat Intelligence

INSERENTENVERZEICHNIS

IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

Chefredaktion: Silvia Parthier (-26)

Redaktion: Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

Autoren: Lars Becker, Philipp von der Brüggen, Abdelghani Faiz, Dr. Thomas Gerick, Kyle Gibbons, Sven Hausen, Thomas Hertel, Ralf Kempf, Prof. Mario Koch, Dr. Georg Kraus, Carina Mitzschke, Angelika Mühleck, Dietmar Nick, Ertan Özdil, Silvia Parthier, Ulrich Parthier, Guido Piech, Moritz Plassnig, Julian Saalfrank, Florian Sackmann, Hanno Scheppig, Dmitrij Spolwind, Anne Teterra, Amadeus Thomas, Ralph Weiss

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Ludwig-Ganghofer-Str. 51, D-83624 Otterfing
Tel: 08104-6494-0, Fax: 08104-6494-22
E-Mail für Leserbriefe: info@it-verlag.de
Homepage: www.it-daily.net

Alle Autoren erreichen Sie über die Redaktion.Wir reichen Ihre Anfragen gerne an die Autoren weiter.

Manuskripteinsendungen: Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmteilen führen, übernimmt der Verlag keine Haftung. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Layout und Umsetzung: K.design | www.kalischdesign.de
mit Unterstützung durch www.schoengraphic.de

Illustrationen und Fotos:
Wenn nicht anders angegeben: shutterstock.com

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 31.
Preisliste gültig ab 1. Oktober 2023.

Mediaberatung & Content Marketing-Lösungen
it management | it security | it daily.net:
Kerstin Fraenzke, 08104-6494-19, fraenzke@it-verlag.de
Karen Reetz-Resch, Home Office: 08121-9775-94, reetz@it-verlag.de
Marion Mann, +49 152-3634 1255, mann@it-verlag.de

Online Campaign Manager:
Roxana Grabenhofer, 08104-6494-21, grabenhofer@it-verlag.de
Head of Marketing:
Vicky Miridakis, 08104-6494-15, miridakis@it-verlag.de

Objektleitung: Ulrich Parthier (-14), ISSN-Nummer: 0945-9650

Erscheinungsweise: 6 x pro Jahr

Verkaufspreis: Einzelheft 20 Euro
Jahresabopreis 100 Euro (Inland), 110 Euro (Ausland)
Probeabo 20 Euro für 2 Ausgaben, PDF-Abo 40 Euro für 6 Ausgaben

Bankverbindung: VRB München Land eG,
IBAN: DE90 7016 6486 0002 5237 52, BIC: GENODEF10HC
Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Abonnementservice: Eva Neff,
Telefon: 08104-6494-15, E-Mail: neff@it-verlag.de
Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Beträge.


e3mag.com
DEUTSCH
Information und Bildungsarbeit von und für die SAP®-Community
The global independent platform for the SAP® community
ENGLISCH
SPANISCH
La plataforma global e independiente para la comunidad SAP®
SAP® ist eine eingetragene Marke der SAP SE in Deutschland und in den anderen Ländern weltweit.


itsa EXPO CONGRESS
PLAY HARD.
PROTECT SMART.
HOME OF IT SECURITY
JETZT GRATIS-TICKET SICHERN!
22. – 24. Oktober 2024
Nürnberg, Germany
itsa365.de/itsa-expo-besuchen
NÜRNBERG MESSE

it security

Detect. Protect. Respond.
Juli/August 2024

THOUGHT LEADERSHIP

AB **SEITE 10**

ninjaOne

CYBER-BEDROHUNGEN

Innovative Lösungen

Axel Unger, NCP engineering GmbH

DATENSPIONE AUSSPERREN

Warum Sie auf CIAM setzen sollten

IDENTITÄTS-MISSBRAUCH

Mit dezentralen Identitäten kontern

CONFIDENTIAL COMPUTING

Darauf hat die Blockchain gewartet

WE SECURE IT

13. und 14. November 2024

Digitalevent

SAVE THE DATE

it-daily.net

#WesecureIT2024

Eine Veranstaltung von itsecurity & it-daily.net

Inhalt

Sichere Kommunikation

INNOVATIVE LÖSUNGEN FÜR NEUE CYBER-BEDROHUNGEN

Die Cybersicherheitsbranche steht angesichts ständig neuer Bedrohungsszenarien vor großen Herausforderungen. Im Interview spricht Axel Unger, Head of R&D bei der NCP engineering GmbH, über die Strategie des Unternehmens und welche Rollen moderne Arbeitsweisen und die richtige Mitarbeiterförderung dabei spielen.

it security: *Herr Unger, wo sehen Sie die aktuellen Herausforderungen in der IT-Branche und wie wirken Sie diesen entgegen?*

Axel Unger: Wir bewegen uns in einem Markt, der stark unter Druck steht. Täglich ist von Cyberattacken zu lesen, die Firmennetzwerke oder gar ganze Kommunen lahmlegen. Glücklicherweise gibt es Antworten auf die gestiegenen Cybersicherheits-Risiken, zum Beispiel Zero-Trust-Ansätze oder SASE.

it security: *Welche Antworten haben Sie bei NCP auf die neue Bedrohungslage?*

Axel Unger: Wir sorgen mit unseren Produkten für eine sichere Kommunikation zwischen Endgeräten und Firmennetzwerken. NCP steht für höchste Qualität in Bezug auf Sicherheit und Zuverlässigkeit bei gleichzeitiger Nutzerfreundlichkeit. All diese Merkmale stehen unter der Marke „Made in Germany" – wir entwickeln und programmieren alle Produkte selbst an unserem Standort in Nürnberg.

it security: *Worauf liegt der Fokus?*

Axel Unger: Der Schwerpunkt liegt auf der Weiterentwicklung unserer Bestandsprodukte: weitere Features, Integrationen oder Komfortfunktionen. Darüber hinaus gibt es jedoch Bereiche, in denen neue Ansätze und Konzepte notwendig sind. Ich denke da an modernen Remote Access, Zero-Trust-Architekturen und SASE-Konzepte, welche den bisherigen Fokus von Perimeterschutz auf die Betrachtung aller Beteiligten verlagern NCP denkt hier nicht dogmatisch, sondern ermöglicht sowohl seinen Bestandskunden so viel wie möglich über die bereits erworbenen Produkte abzubilden, als auch bei neuen Kunden eine schnelle und zielgerichtete Integration für ihre individuellen Sicherheitsanforderungen.

> HEUTE IST ES ESSENZIELLER DENN JE, INDIVIDUELL AUF MITARBEITER EINZUGEHEN.
>
> **Axel Unger, Head of R&D, NCP engineering GmbH, www.ncp-e.com**

it security: *Wo sehen Sie potenzielle Wachstumsmärkte in der IT-Branche?*

Axel Unger: Technologisch gesehen vor allem im Bereich des mobilen Arbeitens. Wirtschaftlich betrachtet ist hier allen voran die USA zu nennen – nicht umsonst hat NCP eine Tochterfirma in Florida und ist damit auch in internationalen Märkten tätig. Unsere Technologie-Partnerschaften mit weltweit führenden Unternehmen wie Aryaka, Juniper Networks, WatchGuard Technologies und Lancom Systems GmbH haben für uns eine große Bedeutung als Impulsgeber für neue Entwicklungen und Produkte. Diese Partner setzen bewusst auf unsere Technologien in ihrem Portfolio.

it security: *Als Leiter für Forschung und Entwicklung bei NCP – wie sehen Sie das Unternehmen aktuell und zukünftig aufgestellt? Welche Aufgaben haben Sie in dieser Rolle übernommen?*

Axel Unger: Grundsätzlich sehe ich NCP mit seinen Produkten mit hoher Produktvarianz als technologischen Marktführer bestens aufgestellt. Wir setzen quasi den De-Facto-Standard für sichere mobile Kommunikation. Die personelle Struktur ist während und nach der Corona-Pandemie bei NCP schnell gewachsen – diese gilt es nun zu organisieren und so effizient wie möglich zu strukturieren. Für mich bedeutet das sowohl die Produktvarianz im Bestandsprodukt als auch die Innovationsfähigkeit in der Neuentwicklung zu ermöglichen.

it security: *Wo liegen Ihrer Meinung nach die Schwierigkeiten einer Neustrukturierung innerhalb einer Entwicklungsabteilung?*

Axel Unger: Ein reibungsloser und effizienter Betrieb steht und fällt mit der Organisation der Zusammenarbeit im Team. Das ist in der Entwicklung nicht anders. Von großer Bedeutung sind organisatorische Maßnahmen wie einfache, klare Abläufe und Verantwortlichkeiten sowie Transparenz in den Inhalten. Zudem sind moderne Arbeitsweisen und Umgebungen Voraussetzung für effizientes Zusammenarbeiten. Dem sind unsere moderne, technologische Umgebung und unsere Arbeitsorganisation basierend auf Kanban bereits gewachsen. Der wesentlichere Teil jedoch ist die Betrachtung der Stärken und Kompetenzen der Mitarbeiter sowie deren gezielte Förderung.

it security:*y: Und wo sehen Sie in Ihrer Abteilung Herausforderungen?*

Axel Unger: Unsere Abteilung besticht durch eine sehr heterogene Zusammensetzung von Kompetenzen, was eine große Vielseitigkeit an Themenstellungen ermöglicht. Gleichzeitig können große Erfahrungsunterschiede und kleinteilige Spezialisierung auch ein Hemmnis für Skalierungsfähigkeit darstellen. Vereinfacht gesagt – es lassen sich mit zu vielen Spezialisten zu wenig Themen gleichzeitig abbilden. Die Herausforderung besteht daher im ersten Schritt in einer Organisation, die Kompetenzübergaben ermöglicht: Aus „Kompetenzinseln" sollen Kompetenzfelder entstehen, die dann sukzessives Wachstum und eine höhere Parallelisierung der Themen erlauben.

it security: *Ihre Herangehensweise setzt ein starkes Team voraus. Nun ist der Personalmangel mittlerweile in allen Branchen angekommen. Wie wirken Sie dieser Entwicklung aktiv entgegen?*

Axel Unger: Das stimmt. Es wird immer schwieriger hochqualifizierte Mitarbeiter zu finden. Es gibt zwar viele gute Entwickler, allerdings können sich diese ihre Jobs mittlerweile weltweit aussuchen. Daher gilt es, als Arbeitgeber attraktiv zu sein und perfekte Rahmenbedingungen zu bieten. Wir bieten einige Stellen speziell in der Entwicklung auch komplett remote an, um ein breiteres Feld an möglichen Interessenten zu erreichen. Außerdem haben wir zahlreiche Benefits, wie zum Beispiel betriebliche Altersvorsorge und Krankenversicherung, Firmenwagen, Job Rad und vieles mehr. Zudem arbeitet unsere Marketing- und PR-Abteilung mit Hochdruck an noch mehr Sichtbarkeit und Präsenz, um potenzielle neue Mitarbeiter zu erreichen.

it security: *Sie sind schon seit einigen Jahren als Führungskraft tätig. Wie hat sich Ihre Rolle in den vergangenen Jahren verändert und warum?*

Axel Unger: Meine Rolle hat sich aufgrund der allgemeinen Entwicklung unserer (Arbeits-)Gesellschaft sehr verändert. Der Fokus liegt heute deutlich klarer darauf, die Zusammenarbeit unter nachvollziehbaren Zielen zu vereinen und Mitarbeitern optimale Bedingungen zu ermöglichen, also den Weg zu ebnen. Dabei ist es heute essenzieller denn je, individuell auf Mitarbeiter einzugehen. Die stark veränderten und unterschiedlichen Bedürfnisse meiner Kollegen spiegeln dabei alle Facetten unserer gesellschaftlichen Entwicklung wider. Remote-Arbeit reflektiert beispielsweise eine neue Balance zwischen Arbeit und Leben, aber auch eine veränderte Haltung zur Mobilität. Die Position als Führungskraft fordert hierbei einen deutlich generalistischen Blick, um Mitarbeitenden gerecht zu werden und motivatorische Aspekte transportieren zu können.

it security: *Was ist für Ihren persönlichen Entfaltungsspielraum besonders wichtig?*

Axel Unger: Für meinen persönlichen beruflichen Alltag ist es sehr wichtig, mit neuen Konzepten und Methoden flexibel auf all diese vielseitigen Veränderungen eingehen zu können. Dafür benötige ich natürlich einen gewissen Spielraum, um entsprechende Entscheidungen zu treffen. So können wir wiederum auf vielleicht noch unbekannte Anforderungen des Marktes frühzeitig eingehen. Außerdem ist es für mich als zweifacher Familienvater wichtig, die Balance zwischen Arbeit und Privatleben zu halten. Die Zeit mit meiner Familie schafft immer einen Ausgleich zum anspruchsvollen Arbeitsalltag. Sport und Bewegung geben mir die notwendige Kraft und Energie.

it security: *Herr Unger, wir danken für dieses Gespräch.*

Business Continuity

WIE IHR UNTERNEHMEN IN 6 SCHRITTEN IMMER PRODUKTIV BLEIBT

Der Begriff „Business Continuity" beschreibt die Fähigkeit eines Unternehmens, sich vor Unterbrechungen des Betriebsprozesses zu schützen, die der Firma ansonsten ernsthafte (wirtschaftliche) Schäden zufügen würden. Wie IDC in ihrer Studie „The Cost of Downtime" herausfand, verursacht ein Infrastrukturausfall Kosten von durchschnittlich 100.000 Dollar – pro Stunde. Sich selbst arbeitsfähig zu halten, sollte für Unternehmen daher einer der wichtigsten Punkte in der Betriebsplanung sein – so zumindest in der Theorie.

Tägliche Herausforderungen gefährden die Produktivität

Dass Business Continuity allerdings nicht immer weit oben auf der Prioritätenliste steht, zeigte die Corona-Pandemie. Durch die Homeoffice-Pflicht waren viele Betriebe gezwungen, ihre Mitarbeiter von heute auf morgen von zuhause aus arbeiten zu lassen. Doch viele waren darauf nicht eingestellt. Dadurch konnten sie nicht sofort auf die neuen Gegebenheiten reagieren, was ihre Produktivität zeitweise minderte und sie gleichzeitig anfälliger für Angriffe von außen machte.

Allerdings muss es nicht gleich eine weltweite Krise sein, die Unternehmen vor unerwartete Herausforderungen in ihrer Produktivität stellt. Auch lokale Ereignisse wie Unwetter oder Blitzeis können jederzeit dafür sorgen, dass Mitarbeiter spontan remote arbeiten müssen. Für solche Fälle ist es im Sinne der Business Continuity, wenn Unternehmen einen Notfallplan und entsprechende Lösungen im Einsatz haben, die sie auch in solchen Situationen voll produktionsfähig halten.

Business-Continuity-Plan

Ein Business-Continuity-Plan umfasst in der Regel folgende Stufen:

Bei der Ausarbeitung ist eine Checkliste nützlich, in der die betreffende Ausstattung und die Standorte von Daten-Backups sowie des Business-Continuity-Plans an sich gelistet sind. Die Kontaktinformationen für Notfallhelfer, Schlüsselpersonal und die Betreiber der Backup-Standorte sollten dort ebenfalls aufgeführt sein. Außerdem sollten auch eine Business-Impact-Analyse sowie der erwähnte Disaster-Recovery-Plan Teil des Business-Continuity-Konzepts eines Unternehmens sein. Diese konzentrieren sich darauf, die essenziellen Prozesse im Unternehmen zu bestimmen, die Ausfallkosten abschätzbar zu machen und die IT-Infrastruktur sowie den laufenden Betrieb nach einem Ausfall wiederherzustellen.

- #1 Den Umfang des Plans bestimmen
- #2 Die wichtigsten Geschäftsbereiche identifizieren
- #3 Zentrale Funktionen festhalten
- #4 Abhängigkeiten zwischen Geschäftsbereichen und Funktionen ermitteln
- #5 Akzeptable Ausfallzeiten und Verluste für jede zentrale Funktion festlegen
- #6 Einen Disaster-Recovery-Plan zur Wiederherstellung nach dem Ernstfall aufstellen

Sicher im Ernstfall

In der Praxis sind für die Umsetzung eines Business-Continuity-Plans auch entsprechende IT-Lösungen notwendig, die dabei helfen, das Unternehmen im Alltag arbeitsfähig zu halten. Dabei kommt es zum einen darauf an, dass die Mitarbeiter ihre Arbeit von überall aus remote verrichten können, und zum anderen, dass die Unternehmens-IT gleichzeitig vor Cyberangriffen geschützt bleibt. Eine moderne Remote-Access-VPN-Lösung ist für die Erfüllung dieser beiden Punkte unverzichtbar.

Bei der Auswahl des richtigen VPN-Produkts können Unternehmen einem 6-Punkte-Plan folgen:

SCHRITT 1:

Ist-Situation analysieren und ein stabiles Fundament schaffen

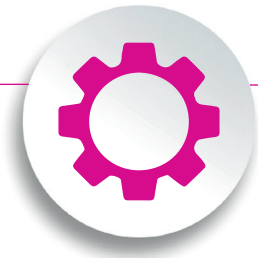
Zu Beginn der Planung sollten einige Fragen geklärt und die Ausgangsituation ermittelt werden. Welche Maßnahmen wurden bereits ergriffen? Wie kann ein sicherer Zugriff auf das Firmennetz aus dem Homeoffice erfolgen? Ist bereits eine Lösung im Einsatz und ist man mit dieser zufrieden? Ist die vorhandene Lösung zukunftssicher und skalierbar sowie an wechselnde Bedarfe anpassbar? Hilfreich ist an dieser Stelle auch das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellte IT-Grundschutz-Kompendium, das zahlreiche Hinweise zu modernen VPN-Lösungen enthält.

>1,25 MRD. DOLLAR

Gesamtkosten für ungeplante IT-Ausfälle pro Jahr

100.000 DOLLAR

Kosten eines Infrastrukturausfalls pro Stunde



>500.000 DOLLAR

Kosten eines kritischen Anwendungsausfalls pro Stunde

SCHRITT 2:

Welche Lösung ist die richtige? Hard- oder Software?

Der Markt an möglichen Lösungen ist kaum zu überblicken. Daher sollten Unternehmen zu Beginn in zwei Kategorien unterscheiden: Hardware-Lösungen, die spezielle Gateway- oder Server-Geräte benötigen, und Software-Lösungen. Generell sind letztere aufgrund ihrer breiten Kompatibilität mit Standard-Hardware/-Betriebssystemen und der sofortigen Verfügbarkeit ohne Lieferengpässe zu empfehlen.

SCHRITT 3:

Administrierbarkeit & Bedienung

Besonders bei hohen Anwenderzahlen ist es unerlässlich, dass die VPN-Lösung einfach zu administrieren bleibt. Dafür sollte der Hersteller ein zentrales Management implementiert haben, welches Administratoren erlaubt, alle Clients aus der Ferne mit Updates und neuen Richtlinien zu versorgen. Außerdem sollten die Clients für Endanwender einfach zu bedienen sein, damit sich diese mit nur einem Mausklick von überall mit der Firmenzentrale verbinden und stabil arbeiten können.

SCHRITT 4:

Wichtige Security-Maßnahmen erfüllen

Neben der reinen Verbindung zum Firmenserver gehört auch der Schutz vor Spionage und Datendieben zur Hauptaufgabe einer VPN-Lösung. Daher sollte diese die hohen deutschen Datenschutzstandards erfüllen und auf technischer Ebene mit Protokollen und Verschlüsselungen wie IPsec und IKEv2 arbeiten.

SCHRITT 5:

Erweiterte Sicherheitsfunktionen

Damit die Datenübertragung aus dem Homeoffice immer sicher abläuft, sind weitere Sicherheitsfunktionen wünschenswert. So sollte die verwendete VPN-Lösung den Verbindungsaufbau mittels Multifaktor-Authentifizierung und weiteren Technologien wie elliptischen Kurven oder digitalen Zertifikaten mehrfach absichern. Außerdem sollten die Geräte der Mitarbeiter und damit auch die Verbindung zur Firmenzentrale über Netzwerkzugriffskontrollen geschützt sein. Diese stellen sicher, dass alle Endgeräte über die aktuellen, sicherheitsrelevanten Softwareversionen verfügen. Abseits dessen sollte eine moderne VPN-Lösung auch über weitere Funktionen wie „Split-Tunneling" und „VPN Bypass" für die Entlastung des Servers sowie „Quality of Service" zur Priorisierung des VoIP-Datenverkehrs verfügen, um sowohl Anwendern als auch Admins das Leben leichter zu machen.

SCHRITT 6:

Die Lösung muss sich dem Bedarf des Unternehmens anpassen, nicht umgekehrt

In Business-Continuity-relevanten Szenarien wird der Bedarf eines Unternehmens für flexiblen Remote Access nie gleichbleiben. So können an „normalen" Tagen wenig VPN-Lizenzen benötigt werden, während im Ernstfall plötzlich ein Großteil der Mitarbeiter remote arbeiten muss. Damit sich ein solches Konstrukt wirtschaftlich sinnvoll betreiben lässt, sollte die VPN-Lösung auch durch ihre Lizenzmodelle skalierbar bleiben. Beliebte Tarifoptionen sind dabei:

- **Pay-per-Use:** Der Kunde erhält eine bestimmte Anzahl an Lizenzen (inkl. Wartung). Es werden jedoch nur so viele Lizenzen abgerechnet, wie der Kunde tatsächlich einsetzt.
- **Temporary Use:** Der Kunde kauft eine bestimmte Anzahl an Lizenzen und bekommt vom Hersteller weitere Lizenzen für eine kurzfristige höhere Nutzung zur Verfügung gestellt. Die Mehrnutzung wird anschließend monatlich abgerechnet.

Folgen Unternehmen den Schritten zum Aufbau eines Business-Continuity-Plans und der Implementierung einer modernen VPN-Lösung, sind sie bestens für etwaige Produktivitätsherausforderungen gerüstet!

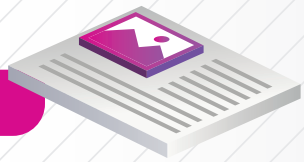
Dennis Christ | www.ncp-e.com

MEHR WERT

Mehr zu „Business Continuity" im Unternehmensumfeld lesen Sie hier

CYBERSECURITY

INNOVATIVE LÖSUNGEN HELFEN



Wenn wir über IT-Security Angriffsvektoren sprechen, dann geht es nicht darum einfach nur ein Problem zu lösen. Es geht darum, dass eine unglaubliche Fülle von Einfallstoren existiert, die mit der jeweiligen, individuellen IT-Infrastruktur abgeglichen, kategorisiert und priorisiert werden muss.

Um dem Ganzen Herr zu werden, bieten Hersteller Innovationen und neue Lösungen, die den Anwendern helfen, ihre Probleme besser, schneller und kostengünstiger zu lösen.

Dieses eBook soll Ihnen dabei helfen, die richtige Lösung zu finden.

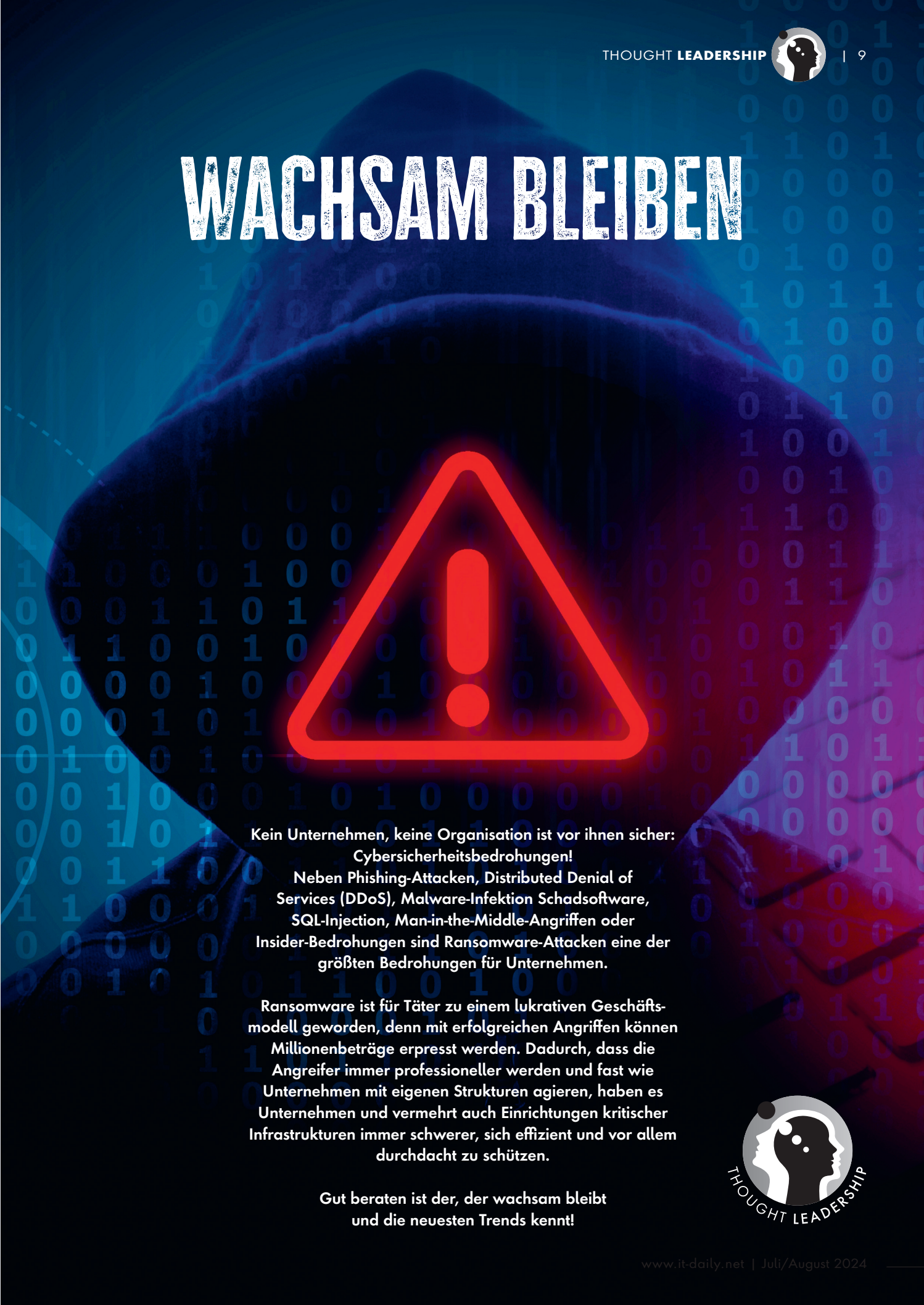
Aus dem Inhalt:

- Valide Sicherheitskontrolle für die Cloud
- Schluss mit Passwörtern
- Passwort Management Lösungen im Überblick
- Passwort knacken? Kein Problem!
- SOAR eine kleine Revolution stellt sich vor
- Security@work
- Cybersecurity auf Applikationsebene
- Digitale Identitäten im Wandel
- Next-Generation EPP
- Generative KI? Aber sicher!
- VPN & die Cloud
- SMTP Smuggling
- Fake-Websites als Köder für Malware

Das **eBook** umfasst 56 Seiten und steht zum kostenlosen Download bereit

www.it-daily.net/download

WACHSAM BLEIBEN



Kein Unternehmen, keine Organisation ist vor ihnen sicher: Cybersicherheitsbedrohungen!
Neben Phishing-Attacken, Distributed Denial of Services (DDoS), Malware-Infektion Schadsoftware, SQL-Injection, Man-in-the-Middle-Angriffen oder Insider-Bedrohungen sind Ransomware-Attacken eine der größten Bedrohungen für Unternehmen.

Ransomware ist für Täter zu einem lukrativen Geschäftsmodell geworden, denn mit erfolgreichen Angriffen können Millionenbeträge erpresst werden. Dadurch, dass die Angreifer immer professioneller werden und fast wie Unternehmen mit eigenen Strukturen agieren, haben es Unternehmen und vermehrt auch Einrichtungen kritischer Infrastrukturen immer schwerer, sich effizient und vor allem durchdacht zu schützen.

Gut beraten ist der, der wachsam bleibt und die neuesten Trends kennt!

THOUGHT LEADERSHIP

Ransomware

DIESE BEST PRACTICES SCHÜTZEN UNTERNEHMEN

WER DIE NEUESTEN TRENDS KENNT, KANN SICH BESSER GEGEN DIE VERHEERENDEN AUSWIRKUNGEN VON RANSOMWARE SCHÜTZEN.

André Schindler, General Manager EMEA, NinjaOne, www.ninjaone.de

Laut BSI (Bundesamt für Sicherheit in der Informationstechnik) und ENISA (Agentur der Europäischen Union für Cybersicherheit) ist Ransomware aktuell die gefährlichste Cyberbedrohung. Entgegen der Annahme, dass solche Angriffe hauptsächlich große Organisationen ins Visier nehmen, sahen Experten 2023 einen signifikanten Anstieg von Attacken auf kleine und mittlere Unternehmen (KMU). André Schindler, General Manager EMEA von NinjaOne, beleuchtet die neuesten Trends in der Ransomware, wirft einen Blick auf die Arbeitsweisen und die Motivation von Ransomware-Gruppen und verrät Best Practices zu Backup-Strategien sowie zur Verteidigung gegen Ransomware-Angriffe.

Neueste Trends im Bereich Ransomware

Ransomware-Angriffe haben sich im Laufe der Jahre erheblich weiterentwickelt. Ursprünglich konzentrierten sich diese Angriffe auf die Verschlüsselung von Daten und das Verlangen eines Lösegeldes für deren Freigabe. Jüngste Trends zeigen jedoch einen Wandel hin zu ausgefeilteren Taktiken, einschließlich Datenexfiltration und verschiedener Erpressungsmethoden. Ransomware-Gruppen stehlen jetzt Daten vor der Verschlüsselung und drohen, sie öffentlich zu machen, wenn das Lösegeld nicht gezahlt wird. Dieser Ansatz, bekannt als doppelte Erpressung, hat den Druck auf die Opfer erhöht, den Lösegeldforderungen nachzukommen, selbst wenn Backups der vertraulichen Daten vorhanden sind.

Darüber hinaus sind Ransomware-Gruppen mit der Zeit professioneller geworden und agieren inzwischen ähnlich wie seriöse Unternehmen. Diese kriminellen Organisationen haben hierarchische Strukturen, spezialisierte Rollen und sogar Kundensupportdienste, um den Opfern bei der Zahlung des Lösegeldes zu helfen. Außerdem hat sich inzwischen das Ransomware-as-a-Service-Modell (RaaS) etabliert, bei dem Entwickler ihre Ransomware-Tools an Partner vermieten, die die Angriffe ausführen. Das hat die Einstiegshürde deutlich gesenkt und so zu einem Anstieg der Zahl der Angreifer sowie der Angriffe geführt.

Die Angreifer: Gut organisiert und gewinnorientiert

Ransomware-Banden sind in erster Linie durch finanziellen Gewinn motiviert. Die Aussicht auf beträchtliche Auszahlungen hat Ransomware zu einer attraktiven Option für Cyberkriminelle gemacht. Diese Banden planen ihre Operationen minutiös und verbringen oft Monate unentdeckt in einem Netzwerk, bevor sie einen Angriff starten. Sie verwenden verschiedene Techniken wie Phishing, das Ausnutzen von Schwachstellen und Brute-Force-Angriffe, um sich zunächst Zugang zu verschaffen. Sobald sie in das Netzwerk eingedrungen sind, bewegen sie sich seitlich durch das Netzwerk, erweitern ihre Privilegien und setzen ihre Ransomware-Payload ein.

Die Opfer: Erst die großen, jetzt die kleinen

Während große Organisationen nach wie vor attraktive Ziele sind, weil sie dazu in der Lage sind, hohe Lösegelder zu zahlen, geraten zunehmend auch KMU ins Visier der Angreifer. Diese kleineren Organisationen verfügen oft nicht über die robusten Sicherheitsmaßnahmen größerer Unternehmen, was sie zu leichteren Zielen macht. H.E.R.O.S., ein Her-

PRAXISBEISPIEL H.E.R.O.S

H.E.R.O.S wurde von einem verheerenden Ransomware-Angriff getroffen, der kritische Daten verschlüsselte und den Betrieb des Unternehmens erheblich störte. Die Organisation nutzte die Backup-Lösung von NinjaOne, die es dem Team ermöglichte, sämtliche Daten schnell und effizient wiederherzustellen, die Ausfallzeit zu minimieren und weitere Verluste zu verhindern. Dieser Fall zeigt die Bedeutung eines zuverlässigen Backupsystems als Teil einer umfassenden Ransomeware-Verteidigungsstrategie.

steller für Helikopterkomponenten, sah sich beispielsweise einem schweren Ransomware-Angriff ausgesetzt. Zwar konnte das Team seine Systeme mit Hilfe einer professionellen Backup-Lösung wiederherstellen. Dennoch macht dieser Fall die Risiken, denen kleinere Unternehmen ausgesetzt sind, und die Bedeutung effektiver Notfallmaßnahmen zur Wiederherstellung deutlich.

Datenexfiltration, doppelte und mehrfache Erpressung

Die Datenexfiltration hat sich zu einer wichtigen Komponente moderner Ransomware-Angriffe entwickelt. Die Angreifer stehlen sensible Daten und drohen damit, sie freizugeben, wenn das Lösegeld nicht gezahlt wird. Zudem können Angreifer gestohlene Daten dank der immer reibungsloser funktionierenden Online-Marktplätze im Darknet monetarisieren. Dadurch kann die Verweigerung der Zahlung des Lösegelds finanziell gut kompensiert werden und Ransomware-Gruppen können ihre Aktivitäten problemlos finanzieren. Diese doppelte Erpressungstaktik erhöht den Einfluss, den die Angreifer auf ihre Opfer haben. In einigen Fällen gehen die Angreifer zu einer Mehrfacherpressung über, indem sie zusätzliche Bedrohungen wie DDoS-Angriffe einsetzen oder Kunden und Partner des Opfers kontaktieren, um den Druck zu erhöhen.

Fazit

Ransomware stellt nach wie vor eine erhebliche Bedrohung für Unternehmen jeder Größe dar. Die zunehmende Raffinesse von Ransomware-Gruppen und ihre sich weiterentwickelnden Taktiken machen es für Unternehmen unerlässlich, wachsam zu bleiben und robuste Sicherheitsmaßnahmen zu implementieren. Wer die neuesten Trends kennt und bewährte Verfahren zur Abwehr und Wiederherstellung anwendet, kann sich besser gegen die verheerenden Auswirkungen von Ransomware schützen.

André Schindler

BEST PRACTICES ZUR VERTEIDIGUNG GEGEN RANSOMWARE

#1 **Regelmäßige Backups:** Stellen Sie sicher, dass Daten regelmäßig gesichert werden und die Backups offline oder in einem anderen Netzwerksegment gespeichert werden, um zu verhindern, dass sie während eines Angriffs verschlüsselt werden.

#2 **Patch-Management:** Halten Sie alle Systeme und sämtliche Software auf dem neuesten Stand, um Schwachstellen zu schließen, die von Angreifern ausgenutzt werden könnten.

#3 **Mitarbeiterschulung:** Führen Sie regelmäßige Trainings durch, um Mitarbeiter über Phishing-Angriffe und andere Social-Engineering-Taktiken aufzuklären.

#4 **Zugriffskontrollen:** Implementieren Sie strenge Zugriffskontrollen und nutzen Sie das Prinzip der minimalen Rechte, um die potenziellen Auswirkungen eines kompromittierten Kontos zu minimieren.

#5 **Endpunktschutz:** Verwenden Sie fortschrittliche Endpoint-Security-Lösungen, die Ransomware erkennen und blockieren können, bevor sie ausgeführt wird.

#6 **Incident-Response-Plan:** Entwickeln Sie einen Incident-Response-Plan und aktualisieren Sie diesen regelmäßig, um eine schnelle und koordinierte Reaktion im Falle eines Angriffs sicherzustellen.

BEST PRACTICES FÜR BACKUP UND RECOVERY

#1 **Isolierung infizierter Systeme:** Isolieren Sie infizierte Systeme schnell, um zu verhindern, dass sich die Ransomware auf andere Teile des Netzwerks ausbreitet.

#2 **Wiederherstellung aus Backups:** Verwenden Sie saubere Backups, um Daten und Systeme wiederherzustellen. Stellen Sie sicher, dass Backups regelmäßig getestet werden, um deren Integrität und Nutzbarkeit zu bestätigen.

#3 **Expertise hinzuziehen:** Holen Sie sich Hilfe von Cybersicherheitsexperten oder Incident-Response-Teams, um Ihre Systeme wiederherzustellen und den Angriff zu untersuchen.

#4 **Kommunikationsplan:** Bereiten Sie einen klaren Kommunikationsplan vor, um Stakeholder, einschließlich Mitarbeitende, Kunden und Partner, über den Angriff und die ergriffenen Maßnahmen zu informieren.

#5 **Nachbearbeitung:** Führen Sie eine gründliche Überprüfung des Vorfalls durch, um die Ursache zu ermitteln und Maßnahmen zur Verhinderung zukünftiger Angriffe zu implementieren.

AUTHENTIFIZIERUNG UND AUTORISIERUNG IN DER IT

GRUNDLAGEN UND KONZEPTE

Das Buch beschreibt grundsätzlich verschiedene Methoden der Authentifizierung und Autorisierung im Rahmen betrieblicher Informationssysteme. Startpunkt ist die Problemstellung, dass Daten und Informationen, Datenflüsse und Informationsflüsse sowohl im Lokalen als auch im Netzwerk geschützt werden müssen. Dazu identifiziert das Buch mehrere Bereiche und Schutzmaßnahmen, wie diese zu kombinieren sind und wie sie sich auf Basis vorhandener Technologien umsetzen lassen. Auch potenzielle Implementierungspattern sind beschrieben.

Sie erfahren, wie Sie Daten insbesondere im Rahmen der DSGVO und der immer stärkeren Verteilung auf Basis von Cloud-native Architekturen schützen können. So reicht es nicht mehr aus, eine einfache Benutzeranmeldung zu implementieren, sondern es müssen auf unterschiedlichsten Ebenen abhängig von der Kritikalität mehr oder weniger umfangreiche und sehr feinmaschige Sicherheitsmechanismen umgesetzt werden.

- die Grundlagen der Authentifizierung und Autorisierung erklärt
- anhand praxisrelevanter Anwendungsfälle dargelegt
- die sinnvollen Lösungsmöglichkeiten erläutert
- effektive Kombinationen und Entscheidungswege beschrieben
- keine bis wenige Vorkenntnisse nötig

Ihr exklusiver Vorteil: E-Book inside beim Kauf des gedruckten Buches.

Authentifizierung und Autorisierung in der IT – Grundlagen und Konzepte; Andreas Lehmann, Mark Lubkowitz, Bernd Rehwaldt; Carl Hanser Verlag GmbH & Co.KG; 02-2024

Aus dem Inhalt:

- Ressourcen schützen
- Anwendungsfälle
- OpenID
- OAuth 2.0
- OpenID Connect
- JSON Web Token
- Policy Enforcement
- Hashfunktionen
- Asymmetrische Verschlüsselung

Quelle: Adobe Stock / ArtemisDiana

CIAM

Sind Sie bereit, mehr darüber zu erfahren, wie Nevis' CIAM-Lösungen die Sicherheit in Ihrem Unternehmen revolutionieren können? Kontaktieren Sie uns unter germany@nevis.net und erfahren Sie aus erster Hand, wie Sie von unseren Technologien profitieren können.

Customer Identity and Access Management

DER SCHLÜSSEL ZUR ABSICHERUNG IHRER DIGITALEN IDENTITÄT

In einer Zeit, in der Cyberangriffe immer raffinierter werden, sind herkömmliche Sicherheitslösungen oft nicht mehr ausreichend. Hier kommt das Customer Identity and Access Management (CIAM) ins Spiel. Die Nevis Security AG, ein führender Anbieter von passwortlosen Authentifizierungslösungen, zeigt fünf Gründe auf, warum CIAM für Unternehmen unerlässlich ist.

#1 Schutz vor ausgeklügelten Cyberangriffen

Cyberkriminelle bieten ihre Dienstleistungen zunehmend als „Crime-as-a-Service" an, was auch weniger versierten Kriminellen Zugang zu ausgeklügelten Angriffstechniken ermöglicht. CIAM-Lösungen von Nevis bieten einen umfassenden Schutz durch Multi-Faktor-Authentifizierung und risikobasierte Authentifizierung, die Phishing-Angriffe und Account Takeovers effektiv verhindern.

#2 Datenschutz und Compliance gewährleisten

Unternehmen stehen unter ständigem Druck, regulatorische Anforderungen und Datenschutzgesetze wie die DSGVO einzuhalten. CIAM hilft, diese Anforderungen zu erfüllen, indem es Datenschutzrichtlinien durchsetzt, Einwilligungsoptionen verwaltet und Audit-Trail-Funktionen bereitstellt. So wird sichergestellt, dass Kundendaten geschützt und die Compliance gestärkt wird.

#3 Zukunftssichere Sicherheitsstrategien entwickeln

Die Verwaltung von Kundenidentitäten erfordert robuste Sicherheitsmaßnahmen. CIAM-Lösungen von Nevis beinhalten Funktionen wie Single Sign-On, Datenverschlüsselung und Zugriffskontrollen, um sensible Informationen zu schützen und Cyberangriffe zu verhindern. Damit wird CIAM zum zentralen Bestandteil jeder zukunftsorientierten Sicherheitsstrategie.

#4 Einsatz von Künstlicher Intelligenz zur Betrugserkennung

Künstliche Intelligenz (KI) spielt eine immer größere Rolle im Bereich des Identitätsmanagements. Nevis setzt KI zur Betrugserkennung und Verhinderung von Account Takeovers ein. Durch den Einsatz von KI-Algorithmen, die Kontextinformationen wie Geolocation und Device-Fingerprint nutzen, wird die Sicherheit erhöht und Prozesse optimiert.

#5 Self Sovereign Identity

Self Sovereign Identity (SSI) gibt Verbrauchern die Kontrolle über ihre Identitätsdaten zurück. Nutzer können Daten in digitalen Geldbörsen speichern und selektiv freigeben. Nevis nutzt diese Prinzipien, um Kunden mehr Kontrolle über ihre Profilinformationen und Autorisierungsrechte zu geben, was den Datenschutz und die Datensicherheit erhöht.

Stephan Schweizer, CEO der Nevis Security AG, betont: „In einem immer wettbewerbsorientierteren Geschäftsumfeld ist Vertrauen die zentrale Grundlage in der Beziehung zwischen Kunden und Unternehmen. Mit einem leistungsstarken CIAM-System können Unternehmen dieses Vertrauen stärken, Cyberkriminalität abwehren und sensible Daten umfassend schützen."

Schützen Sie Ihre digitale Zukunft

Nevis Security bietet mit seinen CIAM-Lösungen eine umfassende Antwort auf die Herausforderungen der Cybersicherheit. Durch den Einsatz von fortschrittlichen Technologien und einem Fokus auf Benutzerfreundlichkeit und Datenschutz hilft Nevis Unternehmen, ihre Sicherheitsstrategien zu optimieren und das Vertrauen ihrer Kunden zu gewinnen.

www.nevis.net

nevis®

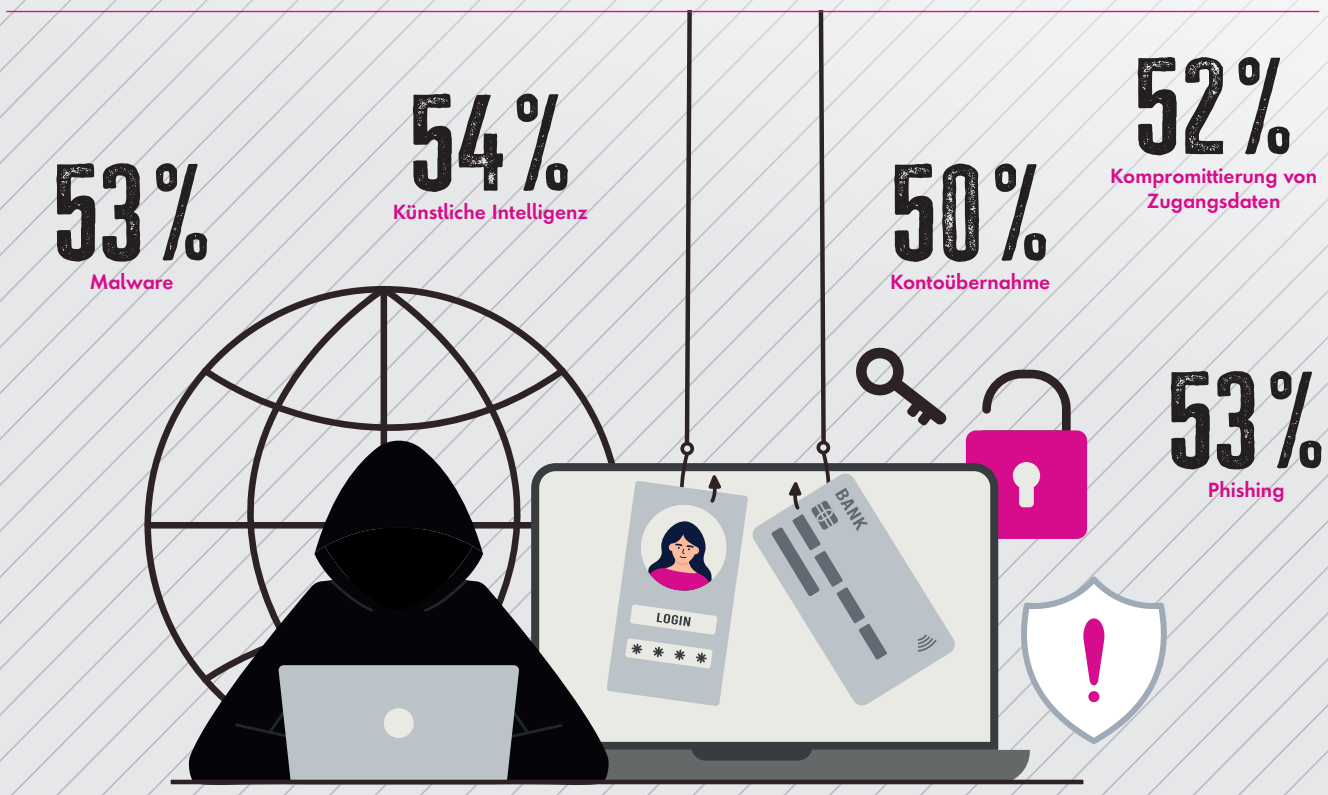
Identitätsmissbrauch

DEUTSCHE GROSSUNTERNEHMEN KONTERN: MIT KI UND DEZENTRALEN IDENTITÄTEN

Seit vielen Jahren schon stellen kompromittierte digitale Nutzeridentitäten für Cyberkriminelle auf der ganzen Welt das primäre Einfallstor in die IT-Systeme ihrer Opfer dar. Getarnt als verifizierte Nutzer spionieren sie deren Systeme aus, platzieren Mal- und Ransomware, tätigen in fremden Namen Bestellungen und Überweisungen. Weltweit sind IT-Sicherheitsexperten überzeugt, dass diese Gefahr in den kommenden Jahren weiter zunehmen wird – nicht zuletzt, da Cyberkriminelle immer häufiger KI-gestützte Tools zur Anwendung bringen. Großunternehmen sind sich der verschärften Risikolage bewusst und haben begonnen, Gegenmaßnahmen einzuleiten – weltweit.

In den vergangenen Jahren und Jahrzehnten haben IAM- und CIAM-Systeme eine rasante Entwicklung durchlaufen. Längst können sie weit mehr als nur ihren Anwendern dabei helfen, digitale Identitätsdaten zu managen und abzusichern. Sie können Unternehmen auch dabei unterstützen, Betrugsversuche präventiv zu verhindern sowie kurativ zu bekämpfen. Jedoch: längst nicht alle Unternehmen haben sich schon zu Investitionen in die neuen Technologien entschließen können. Hauptnutzer sind – derzeit – in aller Regel immer noch diejenigen Unternehmen, die über die meisten Ressourcen verfügen: Großunternehmen. Sie testen aus, stellen die Weichen, geben den Weg vor, den über kurz oder lang dann auch die mittleren und kleinen Unternehmen be-

DIE VIELFALT DER ANSATZPUNKTE ZUM IDENTITÄTSBETRUG BEREITET DER MEHRHEIT DER GROSSUNTERNEHMEN WELTWEIT ERHEBLICHE SORGEN



Quelle: Ping Identity, Fighting The Next Major Digital Threat: AI and Identity Fraud Protection Takes Priority (2024)

schreiten werden. Wie Entscheidungsträger von Großunternehmen die derzeitige Sicherheitslage ihrer digitalen Identitäten einschätzen, welche Maßnahmen sie planen oder bereits ergriffen haben, zeigt die vor kurzem von Ping Identity veröffentlichte Umfrage „Fighting The Next Major Digital Threat: AI and Identity Fraud Protection Takes Priority". Insgesamt 700 ranghohe Entscheidungsträger von Großunternehmen wurden in ihr befragt – darunter auch 100 Vertreter deutscher Großunternehmen.

Digitale Identitäten im Fadenkreuz von Cyberkriminellen

Der Schutz der digitalen Identitäten von Mitarbeitern, Partnern, Zulieferern und Kunden stellt bei der Minimierung der Risiken für die Sicherheit von IT-Systemen, Anwendungen und Daten einen Schlüsselfaktor dar. Schon heute lässt sich die Mehrzahl erfolgreicher Cyberangriffe auf die Kaperung und Kompromittierung von Nutzerkonten zurückführen. Über Social Engineering, Phishing und Spear Phishing bringen sich Cyberkriminelle in den Besitz der Informationen, erstellen Fake Accounts, übernehmen Original-Accounts oder kompromittieren diese.

So schützen sich Großunternehmen

In der Umfrage erklärten über 90 Prozent der befragten hochrangigen IT-Entscheider, die Risikolage ihres Unternehmens in Bezug auf die derzeit gängigen Angriffsvarianten zum Identitätsbetrug – von Credential Compromise, Phishing und Session Hijacking, über Synthetic Entities, Fake Accounts und Account Takeover, bis hin zu Social Engineering – als ‚besorgniserregend' oder sogar ‚sehr besorgniserregend' einzustufen. Kein Wunder! Sind die derzeit vielerorts implementierten Sicherungsmaßnahmen doch meist selbst im Fall von Großunternehmen immer noch stark ausbaufähig. Nur rund 50 Prozent haben bereits eine sichere Zwei- oder gar Multi-Faktor-Authentifizierung implementiert. Nur knapp die Hälfte setzt auf biometrische oder besitzgebundene, ein gutes Drittel immer noch auf – weitaus unsicherere – wissensbasierte Faktoren. Deutsche Großunternehmen sind sogar noch schlechter aufgestellt. Rund die Hälfte nutzt nach wie vor den Faktor Wissen, vertraut zum Beispiel unsicheren Nutzername-Passwort-Kombinationen. Erfreulich ist aber: die Mehrheit – rund 60 Prozent – will in den kommenden 12 Monaten ihre Investitionen in IAM- und CIAM-Systeme erhöhen – von der Betrugsprävention über die Betrugserkennung bis hin zur Betrugsbekämpfung. Im Schnitt sollen 30,5 Millionen Euro investiert werden. In Deutschland liegt dieser Wert sogar noch etwas höher – bei 35,7 Millionen Euro. Doch hängt dies nicht zuletzt auch damit zusammen, dass deutsche IT-Entscheider mehrheitlich auf eigene Inhouse-Lösungen setzen, während international hybriden Lösungen, einer Kombination aus Inhouse- und Anbieter-Lösungen, der Vorzug gegeben wird.

KI – Gamechanger im Missbrauch digitaler Identitätsdaten

Diese Investitionserhöhungen haben sie auch bitter nötig. Denn in den kommenden Jahren werden sich Qualität und Quantität identitätsbezogener Angriffe aller Voraussicht nach signifikant erhöhen. Der Grund: die wachsende Verbreitung KI-gestützter Angriffstools. Mit ihrer Hilfe können Angriffskampagnen automatisiert an spezifische Einzelopfer oder auch Opfergruppen angepasst werden. Deep Fakes, schon heute in aller Munde, werden dann, aller Voraussicht nach, noch einmal einen deutlichen höheren Wirkungsgrad als heute entfalten können. IT-Entscheider von Großunternehmen haben diese Gefährdungsentwicklung erfreulicherweise im Blick. So vertreten über 80 Prozent der Umfrageteilnehmer die Ansicht, dass der Einsatz von KI durch Cyberkriminelle die identitätsbasierte Bedrohungslage in den kommenden 12 Monaten noch einmal drastisch verschärfen wird. Über 90 Prozent stufen ‚neue KI-gestützte Bedrohungen' für ihr Unternehmen als besorgniserregendes oder sogar sehr besorgniserregendes Risiko ein. Entsprechend weit sind hier auch schon die Vorbereitungen zum Umgang mit der verschärften Bedrohungslage vorangeschritten. Rund 40 Prozent haben bereits eine fertige Strategie gegen KI-gestützte Identitätsbedrohungen implementiert. Weitere 40 Prozent haben eine Strategie bereits erarbeitet, müssen sie aber noch implementieren. Und 15 Prozent sind noch mit den Planungen beschäftigt.

DER SCHUTZ DER DIGITALEN IDENTITÄTEN STELLT BEI DER MINIMIERUNG DER RISIKEN FÜR DIE SICHERHEIT VON IT-SYSTEMEN, ANWENDUNGEN UND DATEN EINEN SCHLÜSSELFAKTOR DAR.

Detlev Riecke,
Regional Vice President, Central Europe,
Ping Identity, www.pingidentity.com

Präventive Vorbeugung – Dezentrale Identitäten

Eine Möglichkeit, die verschärfte Identitätsbedrohungslage präventiv anzugehen, stellt der Einsatz dezentraler Identitäten dar. Rund die Hälfte aller Umfrageteilnehmer erklärte, dezentrale Identitäten bereits in den eigenen IAM-

und CIAM-Systemen im Einsatz zu haben. Ein weiteres Drittel gab an, einen Einsatz in den kommenden 12 Monaten anzustreben. Allerdings: Das Gros der Befragten sieht dezentrale Identitäten primär als Mittel zur Lösung von Business-Problemen. Nur eine Minderheit, rund 20 Prozent, glaubt, dass der Einsatz dezentraler Identitäten ihnen dabei helfen wird, Risiken, wie New Account Fraud and Account Takeover, einzudämmen. Hier ist also noch viel Aufklärungsarbeit zu leisten. Sind dezentrale Identitätsmanagementlösungen ihren zentralen Vorläufern doch eben gerade hierin überlegen – in den Bereichen Datensicherheit und Datenschutz – und dies, ohne die Anwenderfreundlichkeit negativ zu belasten.

Kurative Bekämpfung – Künstliche Intelligenz

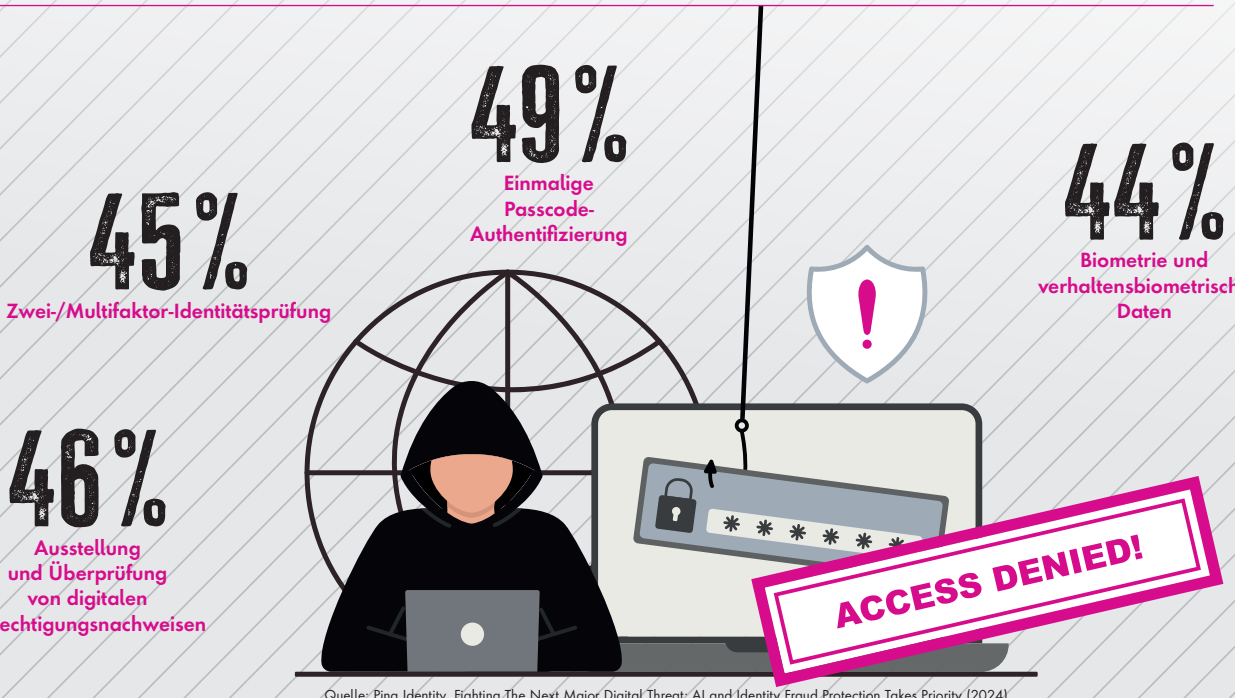
Eine andere Möglichkeit, KI-gestützten digitalen Identitätsbetrug in den Griff zu bekommen: die aktive Aufspürung und Beseitigung betrügerischer Aktivitäten unter Zuhilfenahme von künstlicher Intelligenz. Über 40 Prozent der Umfrageteilnehmer erklärten, sich vom Einsatz künstlicher Intelligenz eine Vereinfachung der Multi-Faktor-Authentifizierung, der Spracherkennung und der Gesichtserkennung zu versprechen. Über 60 Prozent glauben, dass der verstärkte Einsatz von KI es ihnen erlauben wird, ihre Authentifizierungsanforderungen dynamischer zu gestalten – basierend auf dem realen Echtzeit-Verhalten ihrer Nutzer. Und über 50 Prozent gehen davon aus, mittels KI ihre CIAM-Prozesse weiter automatisieren und die automatische Betrugserkennung besser trainieren zu können.

Fazit

Die Ping Identity-Umfrage zeigt, weltweit haben Großunternehmen verstanden, dass sich die identitätsbedingte Risikolage mit der zunehmenden Verbreitung von KI noch einmal deutlich verschärfen wird. Viele haben deshalb begonnen, umfangreiche Investitionen einzuleiten: in neuere und neueste IAM- und CIAM-Technologien – wie KI-gestützte Lösungen zum Aufspüren von Identitätsbetrug und Lösungen zum dezentralen Management digitaler Identitäten. In den kommenden Jahren werden kleine und mittlere Unternehmen hier nachziehen – auch in Deutschland. Den ressourcenintensiven Ansatz vieler Großunternehmen, dabei ganz oder teilweise auf Inhouse-Lösungen zu setzen, werden sich nur die wenigsten von ihnen leisten können. Das wird aber auch gar nicht nötig sein. Denn effektive Anbieter-Lösungen gibt es schon heute. Und in den kommenden Jahren, davon ist auszugehen, werden sie auch für kleine und kleinste Unternehmen immer erschwinglicher werden.

Detlev Riecke

SCHUTZMASSNAHMEN GEGEN IDENTITÄTSBETRUG, DIE BEI GROSSUNTERNEHMEN WELTWEIT AM HÄUFIGSTEN ZUM EINSATZ KOMMEN



Quelle: Ping Identity, Fighting The Next Major Digital Threat: AI and Identity Fraud Protection Takes Priority (2024)

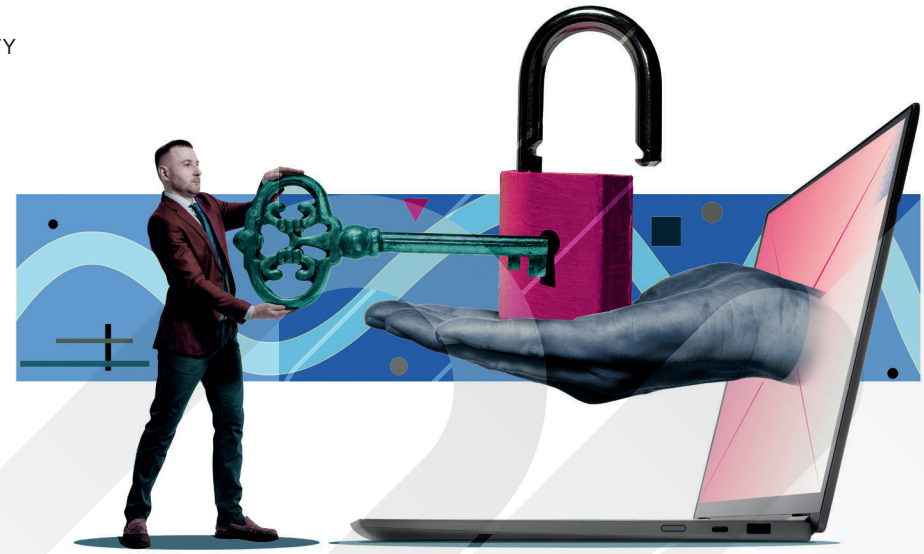
Phi·shing

/'fɪʃɪŋ/

Substantiv, Neutrum [das]

englisch phishing, zu: fishing = das Fischen;
die ph-Schreibung als häufig gebrauchte Verfremdung im Hackerjargon für f wohl nach englisch-amerikanisch phreaking = das Hacken (zu: freak, Freak).

Beschaffung persönlicher Daten anderer Personen (Passwort, Kreditkartennummer o. Ä.) mit gefälschten E-Mails oder Websites.



Datenspione aussperren

WARUM UNTERNEHMEN AUF CIAM SETZEN SOLLTEN

Identitätsdiebstahl und Ransomware sind laut einer aktuellen BSI-Studie die derzeit größten IT-Bedrohungen in Deutschland. Dass es in Sachen Cybersicherheit bei Unternehmen, Behörden und Co. teils riesigen Nachholbedarf gibt, zeigte zuletzt der vielfach diskutierte Daten-Supergau, als der russische Geheimdienst vertrauliche Gespräche der Bundeswehr öffentlich machte.

Wer sensible Informationen wirklich verlässlich vor unbefugten Zugriffen schützen will, benötigt einen Ansatz, der sich an neuartige Angriffe und Szenarien anpasst. Warum an Customer Identity and Access Management (CIAM) 2024 und darüber hinaus kein Weg vorbeiführt.

Passgenauer CIAM-Schutz

Immer professionellere Hacker bieten ihre betrügerischen Dienste auf dem Markt vermehrt auch als „Crime-as-a-Service" (CaaS) an. Ohne besondere IT-Kenntnisse können Kriminelle dadurch betrügerische Aktionen durchführen, was die Effizienz und das Ausmaß der Cyberkriminalität erheblich steigert. Dies zeigt sich beispielsweise auch im Europol-Bericht „Cyber-attacks: the apex of crime-as-a-service". Besonders beliebte Methoden, um in fremde Systeme einzudringen, sind diesem zufolge Phishing-E-Mails mit Malware oder das Ausnutzen von Schwachstellen oder des Remote Desktop Protocol (RDP). Ein gestohlenes Passwort kann genutzt werden, um weitreichendere Kill-Chains zu starten. Um derartige Ketten bereits in ihren Anfängen zu stoppen, rückt CIAM beim Schutz sensibler Daten vermehrt in den Fokus.

WENN FIRMEN UND BEHÖRDEN AUF EIN LEISTUNGSSTARKES CIAM-SYSTEM SETZEN, KÖNNEN SIE DAS VERTRAUEN STÄRKEN, CYBERKRIMINALITÄT DEN RIEGEL VORSCHIEBEN UND SENSIBLE DATEN UMFASSEND SCHÜTZEN.

Stephan Schweizer, CEO, Nevis Security AG, www.nevis.net/de

Datenschutz priorisieren, Compliance stärken

Unternehmen unterliegen zahlreichen regulatorischen Anforderungen und Datenschutzgesetzen, die den Umgang mit Kundendaten regeln. CIAM hilft, Compliance-Anforderungen einzuhalten, indem es ihnen ermöglicht, Datenschutzrichtlinien umzusetzen, Einwilligungsoptionen zu verwalten und Audit-Trail-Funktionen bereitzustellen, um die Nutzung von Kundendaten nachzuverfolgen. Starke Authentifizierungsmethoden wie Zwei-Faktor-Authentifizierung können den Zugang zu Konten erschweren und so Cyberattacken entgegenwirken. Dies unterstützt auch die Einhaltung von Datenschutz- und Sicherheitsstandards.

Zukunftsorientierte Sicherheitsstrategien

Die Verwaltung von Anwender- und Kundendaten sowie Zugriffsrechten erfordert vielfältige und robuste Sicherheitsmaßnahmen, um sensible Informationen vor Verlust und Cyberangriffen zu schützen. Customer Identity and Access Management beinhaltet Funktionen wie Multi-Faktor-Authentifizierung (MFA), Single Sign-On (SSO), Datenverschlüsselung und Zugriffskontrollen, um die Sicherheit persönlicher Daten zu

gewährleisten und die Einhaltung von Datenschutzvorschriften wie der DSGVO sicherzustellen. CIAM ist die essenzielle Basis starker Sicherheitsmaßnahmen gegen unbefugten Datenzugriff oder -verlust, Cyberattacken und mehr.

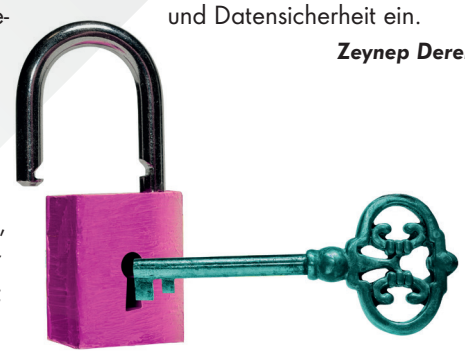
KI-Siegeszug

Laut einer Studie von McKinsey setzt bereits ein Drittel aller befragten Unternehmen weltweit Künstliche Intelligenz ein, Tendenz steigend. Um umfassende Sicherheit zu gewährleisten, ist KI daher ein immer wichtiger werdender Bereich verlässlicher Security-Strategien. Gleichzeitig setzen auch Angreifer vermehrt auf KI. Im Bereich des Identitätsmanagements wird KI künftig ebenfalls eine immer größere Rolle spielen. Bereits heute ist sie hier ein integraler Bestandteil, vor allem bei der Betrugserkennung und der Verhinderung von Account Takeovers (ATO, Kontoübernahmen). Um einen Risikoscore durch KI-Algorithmen zu berechnen, kommen Kontextinformationen wie Geolocation und Device-Fingerprint zum Einsatz. Eine angemessene Anwendung von KI im CIAM kann die Sicherheit erhöhen, Prozesse optimieren und Wettbewerbsvorteile schaffen. Um das Vertrauen der Kunden und Anwender zu stärken, ist hierbei jedoch eine klare Kommunikation zur Funktionsweise von KI-Systemen erforderlich.

Self Sovereign Identity

Den meisten Verbrauchern ist der Schutz ihrer persönlichen Daten heute sehr wichtig - insbesondere, wenn es um ihre E-Mail geht. In einer Nevis-Studie gaben rund 58 Prozent der Privatnutzer an, dass diese für sie besonders schützenswert sei. Self Sovereign Identity (SSI) ermöglicht es, die Kontrolle über eigene Identitätsdaten zu behalten, indem sie beispielsweise in digitalen Geldbörsen gespeichert und selektiv freigegeben werden. Unternehmen können im CIAM-Umfeld die SSI-Prinzipien nutzen, um Kunden die Kontrolle über ihre Profilinformationen und Autorisierungsrechte zu geben. SSI setzt kryptographische Technologien für die Gewährleistung von Datenschutz und Datensicherheit ein.

Zeynep Dereköy



Cybersecurity

ZERO TRUST IN DER CONNECTIVITY CLOUD

Unternehmen bieten zunehmend flexible Arbeitsbedingungen, sodass sich Mitarbeitende an jedem Tag von überall aus einloggen können. Hinzu kommt, dass vielen Mitarbeitenden mehrere Geräte zur Verfügung stehen und sie WiFi mit unterschiedlichen Konnektivitäts- und Internet-Sicherheitsstufen nutzen. Für die Unternehmens-IT bedeutet dies, dass sie nur begrenzt die Kontrolle hat. Was für die Mitarbeitenden ein Plus an Flexibilität bedeutet, ist für die IT-Security ein Albtraum. Cyberpiraten nehmen Mitarbeitende, Teams oder ganze Abteilungen ins Visier und greifen sie in unterschiedlicher Stärke und Komplexität an. Die große Frage:

Wie können Öffentlicher Bereich und Unternehmen sicherstellen, dass ihre Teams wirksam vor potenziellen Cyberschwachstellen geschützt sind?

Tatsächlich müssen Organisationen jeder Größe ihre Sicherheitsvorkehrungen auf dem neuesten Stand halten und neue Maßnahmen ergreifen, um ihre Systeme und Infrastrukturen angesichts der jüngsten Trends in Sachen digitaler Transformation, Remote-Arbeit und anhaltender Entwicklungen zu schützen.

Unabhängig von der Größe oder der Art des Unternehmens ist es ohne einen starken, belastbaren Netzwerkschutz nur eine Frage der Zeit, bis die Systeme kompromittiert werden.

WENN EIN UNTERNEHMEN SEINE NETZWERKSICHERHEIT NICHT REGELMÄSSIG ÜBERPRÜFT, AKTUALISIERT UND VERBESSERT, MACHT ES SICH UNNÖTIG ANGREIFBAR.

Stefan Henke, RVP DACH, Cloudflare GmbH, www.cloudflare.com

Vor allem die Idee des Zero Trust setzt sich in der Sphäre der Cybersicherheit durch. Dem Konzept liegt das Prinzip zu Grunde, keinem Nutzer zu vertrauen, gleich ob dieser remote arbeitet oder sich innerhalb des Netzwerks befindet. Dabei wird jede Anfrage an jede Ressource einzeln überprüft. Bei anderen, traditionellen Formen der Netzwerksicherheit kann sich eine Bedrohung, wenn sie die Schutzmaßnahmen überwindet und in die Systeme eines Unternehmens eindringt, nach Belieben bewegen.

Mehr Sicherheit dank Zero Trust

Durch die Anwendung eines Zero-Trust-Modells wird kein Nutzender automatisch als vertrauenswürdig eingestuft, da davon ausgegangen wird, dass es Bedrohungen sowohl innerhalb als auch außerhalb des Netzwerks gibt. Der Zero-Trust-Ansatz setzt auf eine regelmäßige Überprüfung der Benutzeridentität, der Berechtigungen, der Geräteidentität und der Sicherheit. Die Anmeldung und die Verbindungen werden ständig unterbrochen, sodass sich Nutzende und Geräte regelmäßig neu verifizieren müssen.

Darüber hinaus können diejenigen, die einen Zero-Trust-Ansatz einführen, eine kontinuierliche Überwachung und Validierung anbieten, um den Zugang zum Netzwerk zu kontrollieren und zu begrenzen. Möglich wird dies durch die Umsetzung der wichtigsten Prinzipien der Zero Trust-Sicherheit: Begrenzung von Zugriffsberechtigungen, Mikro-Segmentierung und Multi-Faktor-Authentifizierung (MFA).

Einfach und schnell

Mitarbeitende sehnen sich nach einer einfachen und schnellen Nutzererfahrung, sei es bei der Anmeldung, der Freigabe von Dateien oder der Einrichtung ihrer Geräte am ersten Tag; veraltete und unwirksame Sicherheitsmaßnahmen bremsen uns nur aus, egal in welcher Rolle. Niemand will das. Der wichtigste Grund für die Implementierung eines Zero-Trust-Modells ist, dass wir jedem, überall und auf jedem Gerät Sicherheit bieten wollen. Zero Trust reduziert den Zeitaufwand für manuelle Sicherheitsaufgaben erheblich, verringert die Angriffsfläche und führt letztlich zu einer höheren Produktivität im

Team, da Zeit zurückgewonnen wird, die sonst für veraltete Sicherheitsmaßnahmen aufgewendet werden müsste.

Aus diesen Gründen beobachten wir eine Veränderung in den Sicherheitsprotokollen der Unternehmen; die klassische perimeterbasierte Netzwerkumgebung („Burg und Burggraben") existiert nicht mehr, das alte Passwort ist fast überholt und VPNs sind zunehmend überflüssig. Warum? Weil wir in der Lage sein müssen, uns überall und schnell zu verbinden, um Arbeitskräften Freiheit zu bieten und den Arbeitsablauf zu verbessern.

Schulungen sind essentiell

Vorbei sind die Zeiten, in denen IT- und Sicherheitsexperten die einzigen Mitarbeitenden waren, die das Netzwerk und seine Bedrohungen verstehen mussten. Wir leben in einem Zeitalter, in dem Mitarbeitende mehr als nur „Computerkenntnisse" haben müssen, um ihr Unternehmen und ihre Netzwerke zu schützen. Die Mitarbeitenden können die erste und letzte Verteidigungslinie sein, wenn es um Cyberbedrohungen geht; Unternehmen sind deshalb gut beraten, eine Kultur der Cybersicherheit zu schaffen und zu kultivieren – vor allem, wenn man bedenkt, dass sich die Cybersicherheit am Arbeitsplatz ständig weiterentwickelt.Die Sicherheitsvorteile des ZT-Modells sind klar, allerdings müssen die Mitarbeitenden über den Zweck des Einsatzes in ihrem Netzwerk geschult werden.

Um daraus Kapital zu schlagen, müssen Investitionen in und Schulungen für Mitarbeitende, die ihr Netzwerk und die Cybersicherheit verstehen, Priorität haben, um das Netzwerk insgesamt zu stärken und unnötige Schwachstellen zu beseitigen. Die Mitarbeitenden sollten regelmäßig über den Einsatz von und die Gründe für Zero Trust unterrichtet werden, insbesondere darüber, dass die getroffenen Maßnahmen dem Schutz und nicht der Überwachung dienen.

Letztlich geht es darum, ein Umfeld zu schaffen, in dem die Mitarbeitenden die Vorteile verstehen und selbstständig handeln können.

Cloudflare One ist die Zero Trust Lösung, als Teil der Connectivity Cloud, die verifiziert, filtert, isoliert und den gesamten Netzwerk-Traffic inspiziert – alles auf einer einheitlichen und kompatiblen Plattform für eine einfache Einrichtung und Bedienung. Ein sicheres virtuelles Backbone, das ein globales Netz von 320 Städten mit über 13.000 Verbindungen nutzt, bietet im Vergleich zum öffentlichen Internet erhebliche Vorteile in Bezug auf Sicherheit, Performance und Zuverlässigkeit.

Stefan Henke

Stärkere Abwehr für Digitalisierung und KI

WIDERSTANDSFÄHIG IN DIE ZUKUNFT DANK NIS2

Kaum ein Thema wird aktuell so intensiv in der IT-Branche diskutiert wie NIS2. NIS2 mag mit seinen strengen Regeln und möglichen Strafen bürokratisch erscheinen, ist aber in Wirklichkeit ein Aufruf zur Stärkung der Abwehr von Cyberbedrohungen: Dies ist eine Chance, die Cyberabwehr und die Widerstandsfähigkeit für ein sicheres digitales Zeitalter mit der Einführung der Richtlinie zur Netz- und Informationssicherheit in Europa zu verbessern.

Network Access Control (NAC) wird bei der Umsetzung von NIS2 eine entscheidende Rolle spielen. Da Unternehmen mit immer komplexeren Cyber-Bedrohungen konfrontiert sind, bieten Lösungen, wie Belden´s macmon NAC, einen soliden Rahmen, um sicherzustellen, dass nur autorisierte und konforme Geräte auf Netzwerkressourcen zugreifen können, und schützen so kritische IT- und OT-Infrastrukturen.

Im Rahmen der NIS2-Richtlinie sind Organisationen verpflichtet, eine Reihe von Maßnahmen zu ergreifen, um die Sicherheit und Widerstandsfähigkeit ihrer Netzwerke und Informationssysteme zu gewährleisten. Diese Maßnahmen umfassen:

#1 **Risikomanagement:** Organisationen müssen einen risikobasierten Ansatz für die Netzwerk- und Informationssicherheit verfolgen. Dieser Ansatz beinhaltet die Identifizierung potenzieller Bedrohungen, die Bewertung ihrer Auswirkungen und die Umsetzung geeigneter Maßnahmen zur Risikominderung. Es ist wichtig, diesen Prozess regelmäßig zu überprüfen und zu aktualisieren, um der sich entwickelnden Bedrohungslandschaft Rechnung zu tragen.

#2 **Technische und organisatorische Maßnahmen:** Die NIS2 verlangt von Organisationen, dass sie geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit ihres Netzwerks und ihrer Informationssysteme zu schützen. Diese Maßnahmen sollten in einem angemessenen Verhältnis zu den festgestellten Risiken stehen und den neuesten Stand der Technik im Bereich der Cybersicherheitstechnologien und -praktiken berücksichtigen. Beispiele für solche Maßnahmen sind Verschlüsselung, Zugangskontrolle, Netzwerksegmentierung und kontinuierliche Überwachung.

#3 **Meldung von Vorfällen:** Organisationen sind verpflichtet, alle

bedeutenden Cyber-Vorfälle, die sich auf die Sicherheit ihres Netzes und ihrer Informationssysteme auswirken, den von ihnen benannten nationalen Behörden zu melden. Die Meldung sollte rechtzeitig erfolgen und ausreichende Informationen enthalten, damit die Behörden den Vorfall bewerten und falls nötig Unterstützung leisten können.

Sichere Netzwerke

Neben den „bekannten" Cyberrisiken hat sich durch das Thema Künstliche Intelligenz eine neue Dynamik in der Cybersecurity entwickelt, denn KI wird branchenübergreifend immer mehr zum Treiber der Digitalisierung. Im Hinblick auf die Einführung von Künstlicher Intelligenz (KI) kann ein vulnerables Netzwerk ernsthafte Probleme verursachen:

- **Cyberangriffe:** Unsichere Netzwerke sind ein Einfallstor für Cyberkriminelle. KI-Systeme können Ziel von Angriffen wie Ransomware, Denial-of-Service (DoS) und Phishing werden.

- **Reputationsschaden:** Ein Sicherheitsverstoß kann zu einem erheblichen Rufschaden für Unternehmen führen. Dies kann Kunden, Investoren und Geschäftspartner abschrecken.

- **Vertrauensverlust:** Wenn KI-Systeme auf unsicheren Netzwerken basieren, verlieren Benutzer und Stakeholder das Vertrauen in die Ergebnisse. Dies kann die Akzeptanz und den Nutzen von KI reduzieren.

- **Regulatorische Probleme:** Unsichere Netzwerke können gegen Datenschutz- und Sicherheitsvorschriften verstoßen. Dies kann zu rechtlichen Konsequenzen führen.

- **Datenverlust und -manipulation:** Unsichere Netzwerke sind anfällig für Datenlecks und -manipulation. KI-Modelle basieren auf riesigen Datenmengen, und wenn Daten gefährdet sind, kann dies zu fehlerhaften Vorhersagen und Entscheidungen führen.

Aufrechterhaltung der Integrität

NAC setzt Sicherheitsrichtlinien durch, die den Zugriff von Geräten auf IT und OT-Netzwerke kontrollieren. NAC-Systeme sind in der Lage, die Konformität eines Geräts mit den Sicherheitsrichtlinien zu bewerten, bevor es eine Verbindung herstellen darf und kontinuierlich, nachdem es eine Verbindung hergestellt hat. Dies ist von entscheidender Bedeutung für die Aufrechterhaltung der Integrität des Netzwerks einer Organisation, insbesondere für Betreiber kritischer Infrastrukturen (KRITIS).

NAC trägt zu den Zielen von NIS2 bei, indem es Folgendes bietet:

- **Identifizierung und Authentifizierung:** NAC-Systeme identifizieren und authentifizieren Geräte, die versuchen, sich mit dem Netzwerk zu verbinden, und stellen so sicher, dass nur Personen mit legitimen Zugangsdaten Zugang erhalten.

- **Durchsetzung von Richtlinien:** NAC ermöglicht Unternehmen die Durchsetzung von Sicherheitsrichtlinien in ihren Netzwerken und stellt sicher, dass Geräte den neuesten Sicherheitsstandards entsprechen.

- **Reaktion auf Vorfälle:** Im Falle eines Sicherheitsverstoßes können NAC-Systeme helfen, den Vorfall einzudämmen, indem sie gefährdete Geräte isolieren und so die Ausbreitung der Bedrohung verhindern. (Segmentierung)

- **Sichtbarkeit und Überwachung:** NAC-Lösungen bieten einen Überblick über die mit dem Netzwerk verbundenen Geräte (Topologie), ihren Konformitätsstatus und ihre Zugriffsmuster, was für die Überwachung und Berichterstattung unerlässlich ist.

NAC – Eckpfeiler der Cyber-Sicherheit

Durch die Integration von NAC in ihre Cyber- und KI-Sicherheitsstrategie können Unternehmen eine proaktive Haltung gegenüber Cyber-Bedrohungen einnehmen. Die Fähigkeit von NAC, den Zugriff auf der Basis von Gerätekonformität und -verhalten zu kontrollieren, steht im Einklang mit dem Ziel der NIS2-Richtlinie, ein hohes gemeinsames Niveau an Cybersicherheit in Europa zu erreichen. Sie unterstützt auch die Forderung der Richtlinie nach strengeren Sicherheitsanforderungen und harmonisierten Durchsetzungsmaßnahmen.

Netzwerksicherheit fördert eine Kultur der Einhaltung und kontinuierlichen Überwachung, die in der dynamischen Landschaft der Cyber-Bedrohungen unerlässlich ist. Die Unternehmen können ihre Sicherheitsmaßnahmen in Echtzeit anpassen und auf neue Schwachstellen und Bedrohungen reagieren, sobald sie auftreten.

Netzwerksicherheit

Zusammenfassend lässt sich sagen, dass NAC nicht nur ein Werkzeug für die Netzwerksicherheit ist, sondern ein strategischer Vorteil, der Unternehmen dabei helfen kann, die strengen Anforderungen der NIS2-Richtlinie zu erfüllen. Ihre zentrale Rolle bei der Identifizierung, Authentifizierung und Durchsetzung der Konformität macht sie zu einem unverzichtbaren Werkzeug für jede Organisation, die sich effektiv und sicher im komplexen Cybersicherheitsökosystem der Europäischen Union bewegen will. NAC sollte daher, als Eckpfeiler eines jeden Cybersicherheitsrahmens betrachtet werden. Außerdem ist eine ganzheitliche Sicherheitsstrategie, die Netzwerksicherheit und KI kombiniert, unerlässlich, um die Vorteile von KI innerhalb der Digitalisierung optimal zu nutzen und gleichzeitig Risiken zu minimieren.

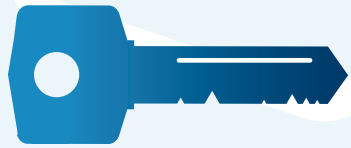
Sabine Kuch | www.macmon.eu

FIDO2-Sicherheitsschlüssel

EFFEKTIVE LÖSUNG FÜR MULTI-FAKTOR-AUTHENTIFIZIERUNG

Mit der EU-Richtlinie NIS2 sollen kritische Infrastrukturen und wichtige digitale Dienste besser vor Cyberbedrohungen geschützt werden. In diesem Zusammenhang wurde der Kreis der „KRITIS-Unternehmen" deutlich erweitert. Allein in Deutschland sind rund 29.000 Organisationen hinzugekommen.

Unabhängig vom Inkrafttreten der nationalen Gesetzgebung gilt die NIS2-Richtlinie unmittelbar ab dem 18. Oktober 2024, selbst wenn nationales Recht noch nicht umgesetzt ist. Eine



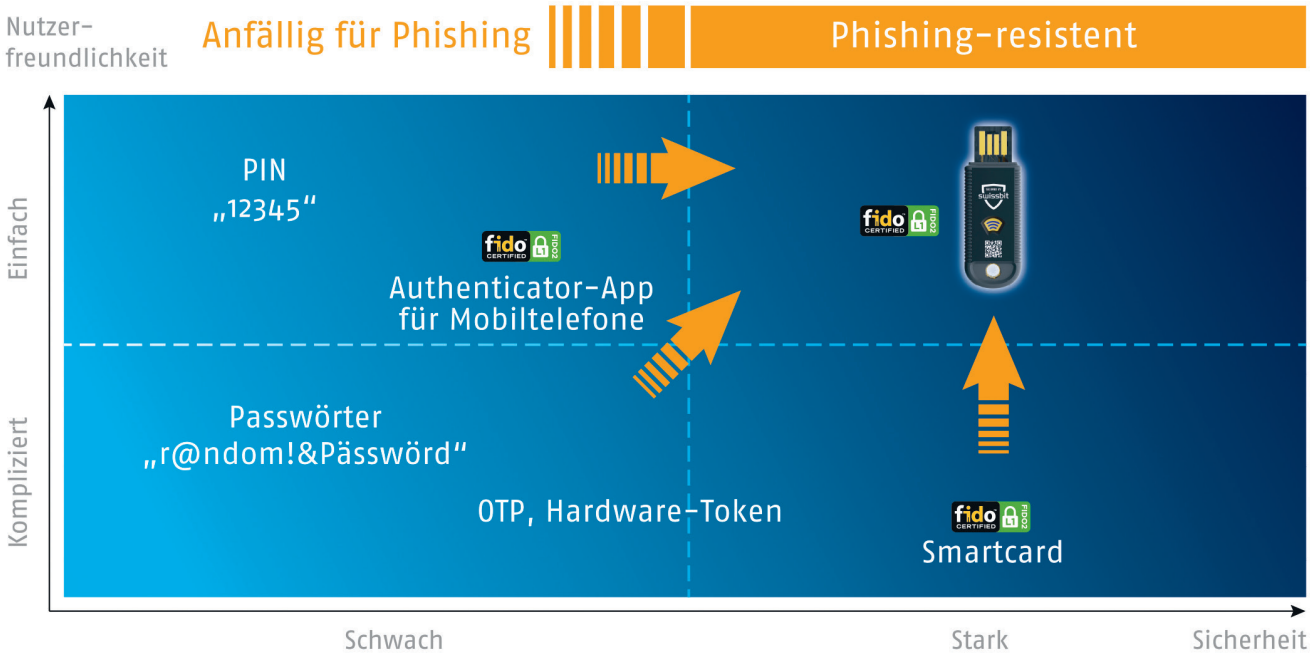
der innerhalb der NIS2 geforderten Maßnahmen ist die Zugriffskontrolle. Viele EU-Länder, darunter auch Deutschland, werden hierfür eine Multi-Faktor-Authentifizierung (MFA) vorschreiben. Dieses Verfahren hat sich als besonders effektiv erwiesen, weil es sich nicht allein auf Wissensfaktoren wie PINs oder Passwörter stützt, sondern weitere Faktoren wie Besitz oder biometrische Merkmale fordert. Besitzkomponenten können hardwarebasiert sein, zum Beispiel ein USB-Token, eine Smartcard oder ein Smartphone. Softwarebasierte MFA-Lösungen nutzen hingegen Smartphone-Apps, SMS oder E-Mails zum Versenden generierter Zugriffscodes.

Smartphone oder FIDO2-Stick?

Klar ist: Passwörter zur Authentisierung reichen längst nicht mehr aus. Sie können durch Phishing und Social-Enginee-

VOR- UND NACHTEILE UNTERSCHIEDLICHER MFA-VERFAHREN

Quelle: Swissbit



ring-Attacken ausgespäht, bei mangelnder Komplexität sogar erraten werden. Eine Authentisierung sollte stattdessen immer mehrere Faktoren umfassen. Neben dem Faktor des geheimen Wissens, sprich des Passworts, kommt dabei mindestens ein zweiter Faktor hinzu. Mobiltelefone scheinen aufgrund ihrer weiten Verbreitung gut geeignet zu sein. Manche Mitarbeiter möchten aber weder ihre privaten Smartphones zur Authentifizierung im beruflichen Kontext nutzen noch dienstliche Smartphones annehmen – abgesehen davon, dass die Anschaffung in der Regel größere Investitionen erfordert und angesichts schneller Modellwechsel keine nachhaltige Lösung darstellt. Wesentlich einfacher ist es, auf FIDO2-Sicherheitsschlüssel wie zum Beispiel den iShield Key Pro von Swissbit zu setzen. Der weltweit verbreitete Standard FIDO2 (Fast IDentity Online) ermöglicht sichere Anmeldeverfahren für Computersysteme, Unternehmensnetzwerke, Websites und Apps. FIDO2 ist eine Initiative der FIDO-Allianz mit dem World Wide Web Consortium (W3C), die von Unternehmen wie Apple, Microsoft und Google unterstützt wird.

Geschäftsführung in der Pflicht

Die Umsetzung von NIS2 in nationales Recht nimmt die Geschäftsführung von KRITIS-Unternehmen persönlich in die Pflicht, ihre IT-Systeme vor unberechtigten Zugriffen zu schützen. Die Erfahrungen der letzten Jahre mit der Datenschutz-Grundverordnung zeigen, dass bei Verstößen nicht mit Nachsicht zu rechnen ist. Betroffene Unternehmen sollten jetzt handeln, um Fristen einzuhalten und empfindliche Strafen zu vermeiden. Wer beim wichtigen Thema NIS2 Multifaktor-Authentifizierung rechtlich, technisch und wirtschaftlich auf der sicheren Seite sein will, ist mit FIDO-Sticks wie dem iShield Key Pro gut beraten. Diese sind nicht nur deutlich kostengünstiger und einfacher zu bedienen als Smartphone-basierte Lösungen, sondern bieten auch die größtmögliche Sicherheit.

Alexander Summerer
www.swissbit.com

IDENTITÄTSBEZOGENE ANGRIFFE

POTENZIELLE BEDROHUNG?

Der aktuelle „CyberArk 2024 Identity Security Threat Landscape Report" zeigt, dass die steigende Zahl menschlicher und nicht-menschlicher Identitäten die Gefahr von Cyberangriffen erhöht. Zudem geht die Studie auf die zunehmende Bedeutung der Künstlichen Intelligenz ein, die einerseits zwar die Cyberabwehr verbessert, andererseits aber Angreifern neue Möglichkeiten eröffnet.

In nahezu jedem Unternehmen sind immer mehr menschliche und vor allem auch nicht-menschliche Identitäten vorhanden. Die Sicherheitsverantwortlichen der befragten Unternehmen in Deutschland stufen dabei nicht-menschliche Identitäten (oft auch als „technische Accounts" bekannt) als den riskantesten Identitätstyp ein. Gründe dafür sind die weit verbreitete Umsetzung von Multi-Cloud-Strategien und die zunehmende KI-Nutzung, die die Zahl von nicht-menschlichen Identitäten deutlich erhöhen. Viele dieser Identitäten erfordern privilegierte Zugriffe. Im Gegensatz zur Verwaltung des menschlichen Zugriffs auf vertrauliche Daten fehlt es bei nicht-menschlichen Identitäten jedoch häufig an Identitätssicherheitskontrollen, sodass sie eine potenzielle Bedrohung darstellen.

www.cyberark.de

85%

der Unternehmen hatten im vergangenen Jahr zwei oder mehr identitätsbezogene Sicherheitsverletzungen

Die Cyberresilienz stärken

WAS UNTERNEHMEN AUS DER DSGVO FÜR DORA UND NIS2 ÜBERNEHMEN KÖNNEN

Die EU setzt mit NIS2 und DORA konsequent fort, was mit der DSGVO begonnen wurde. Sie reguliert die Datenindustrie und die digitalen Prozesse zahlreicher Unternehmen, um die Widerstandsfähigkeit von Daten und Netzwerken gegen Angriffe zu erhöhen. Aus der Einführung der DSGVO lassen sich zudem wichtige Erkenntnisse für den Umgang mit den neuen Regelungen ableiten.

„Und der Haifisch, der hat Zähne und Mekki Messer hat ein Messer. Aber ob die DSGVO Zähne haben wird oder die Folgen für Firmen eher unsichtbar sein werden, wenn sie gegen die Vorgaben verstoßen? Das war die große Frage bei der Einführung am 24. Mai 2018.

Werden die angekündigten Sanktionen durchgesetzt und wenn ja, wie streng?

Nach sechs Jahren gibt der Enforcement Tracker ein deutliches Bild ab. Er listet alle bisherigen Verfahren und verhängten Bußgelder auf. 4,5 Milliarden Euro Bußgelder wurden bisher im Jahr 2024 ausgesprochen, eine halbe Milliarde mehr als 2023 zur gleichen Zeit. Ein Anstieg von 11 Prozent innerhalb von 12 Monaten. Die globale Anwaltskanzlei DLA Piper geht in ihrer jährlichen Studie vom Januar 2024 zu Bußgeldern und Datenschutzverletzungen sogar von einem Anstieg von 14 Prozent aus. DLA Piper hat darin ebenfalls festgestellt, dass sich der Trend der vergangenen Jahre fortsetzt: Wurden in Deutschland 2022 durchschnittlich 328 Verstöße pro Tag gemeldet, waren es im vergangenen Jahr 335 Meldungen – ein konstant hoher Wert. Wenn Firmen die personenbezogenen Daten der EU-Bürger unsachgemäß verarbeiten, werden sie gemeldet und im Ernstfall abgestraft.

Mehr operative Cyberresilienz

Aktuell will die EU mit weiteren neuen Regelungen dafür sorgen, dass Firmen nicht nur ihren Umgang mit Daten optimieren, sondern auch ihre IT operativ besser aufstellen, um Cyberangriffen stärker zu widerstehen. Mit dem Digital Operational Resilience Act (DORA), auf die Finanzindustrie fokussiert, und der NIS2 Directive sind Regelwerke entwickelt worden, um von Firmen in Europa mehr operative Cyberresilienz zu fordern.

DORA wird am 17. Januar 2025 scharf geschaltet, während NIS2 bereits bis spätestens 17. Oktober 2024 relevant wird. Einige europäische Länder sind schon weit fortgeschritten und werden ihre lokalen Gesetze vor diesem Stichtag verabschieden. Wer als Firma in diesen europäischen Ländern geschäftlich aktiv ist, muss also früher auf die Vorgaben reagieren, auch wenn die deutsche Gesetzgebung noch nicht fertig ist.

Die EU hat wie bei der DSGVO auch bei diesen neuen Regelwerken signifikante Bußgelder für Verstöße vorgesehen. Kommen Firmen ihren DORA-Verpflichtungen nicht nach, drohen Bußgelder von bis zu 10 Millionen EUR

oder 5 Prozent des weltweiten Vorjahresumsatzes. Die Strafen bei NIS2 sind nochmal schärfer und nehmen die Geschäftsleitung nun stärker ins Visier. Die Geldbußen können von 100.000 Euro bis zu 20 Millionen Euro für juristische Personen erreichen. Die Bußgelder haben sich seit dem IT-Sicherheitsgesetz 2.0 aus dem Jahr 2021 bei Verstößen deutlich erhöht. Es ist zudem zu erwarten, dass die Behörden Verstöße ähnlich konsequent verfolgen werden, wie sie es bei der DSGVO tun.

Wie NIS2 und DORA zusammenhängen

NIS2 erweitert die Menge der Industriesektoren, die der Vorgabe folgen müssen, drastisch im Vergleich zum Vorgänger von 2016. In Deutschland allein ist mit knapp 30.000 Firmen der Großteil der Wirtschaft betroffen - mit Ausnahme des Finanzmarkts. Dieser wird vorrangig von DORA reglementiert, man spricht hier von einer Lex Specialis. Wichtig ist zu wissen: In all den Fällen, in denen NIS2 Bereiche reguliert, die in DORA ausgespart wurden, ist NIS2 zu betrachten. Letztere füllt also die Aussparungen von DORA, beide hängen zusammen.

Die große Änderung bei den Vorgaben betrifft die obligatorischen Meldepflichten für Datenschutzverletzungen. Im Rahmen der Richtlinie werden die folgenden Anforderungen festgelegt:

- Innerhalb von 24 Stunden muss die Organisation eine Frühwarnung geben, wenn der Verdacht besteht, dass ein schwerwiegender Vorfall durch rechtswidrige oder böswillige Handlungen verursacht wurde oder grenzüberschreitende Auswirkungen haben könnte.

- Innerhalb von 72 Stunden nach Bekanntwerden eines schwerwiegenden Vorfalls muss die Frühwarnung mit einer ersten Bewertung, einschließlich seiner Schwere und Auswirkungen, aktualisiert werden. Die Organisation sollte dem nationalen CERT auch alle Indikatoren für eine Gefährdung im Zusammenhang mit dem Angriff mitteilen.

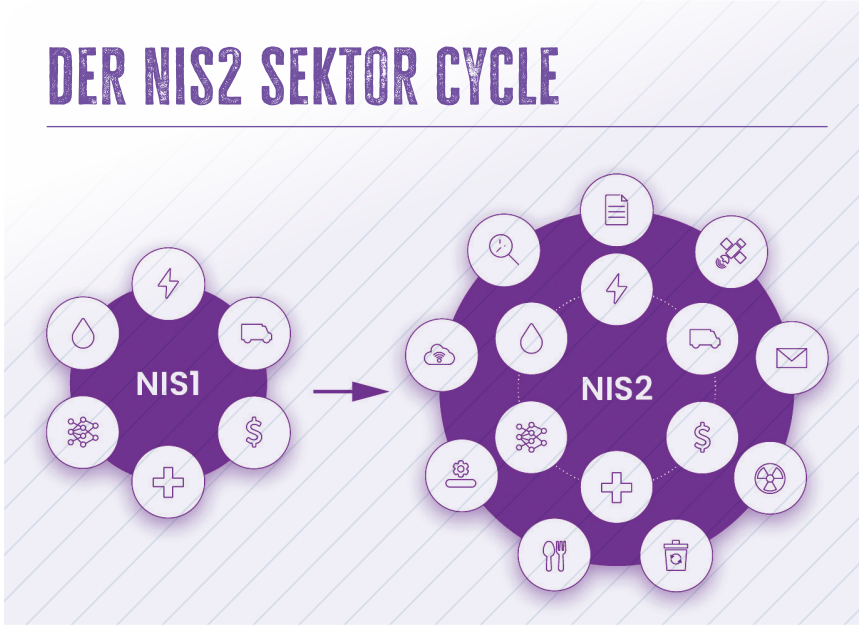
- Auf Anfrage eines nationalen CERT oder einer Aufsichtsbehörde muss die Organisation Zwischenstatusaktualisierungen bereitstellen.

- Innerhalb eines Monats nach Einreichung der Vorfallmeldung muss die Organisation einen Abschlussbericht vorlegen.

Von Vorarbeiten bei der DSGVO profitieren

Die DSGVO hat von Firmen bereits ein besseres Datenmanagement verlangt, indem die Firmen personenbezogene Daten strenger und sorgfältiger verwalten mussten als alle anderen Informationen. Die Auskunftspflicht wie das Recht auf Vergessen sowie die Meldepflicht bei Datenverlust haben von Unternehmen bereits Prozesse und Workflows gefordert, die in ähnlicher Weise bei NIS2 und DORA im Falle eines Angriffs greifen können. Der Einsatz einer KI-getriebenen Data-Security- und Management-Plattform kann Firmen immens helfen, diese Prozesse skalierbar und effizient im Unternehmen umzusetzen.

Dateninhalte genau kennen: Bei einer Attacke wollen die Hacker Daten stehlen, verschlüsseln oder löschen. Unternehmen müssen daher genau wissen, welche Daten sie besitzen und welchen Wert sie haben. Nur dann können sie Fragen der Governance und Compliance beantworten und beispielsweise steuern, dass bestimmte Datentypen gewisse Speicherorte nicht verlassen dürfen. Und sie werden schneller verstehen, welche Daten im Detail betroffen sind, sollten Hacker erfolgreich eingedrungen sein. Dadurch wird das Reporting für NIS2 und DORA beschleu-



nigt und die Ergebnisse viel genauer. Im Alltag ist diese Aufgabe gigantisch und die meisten Firmen haben Berge von Informationen angehäuft, von denen sie wenig bis überhaupt nichts wissen. Auf diesem Gebiet können KI-Lösungen wie Cohesity Gaia massiv helfen und eine der komplexesten Probleme entschärfen, indem sie die Daten von Firmen automatisiert klassifizieren. Business Owner können beispielsweise direkte Fragen zu bestimmten Daten stellen und bekommen automatisch von Gaia eine entsprechende Antwort mit einer Liste aller betroffenen Dokumente.

Da Cohesity die Daten aus dem eigenen Backup klassifiziert, lassen sich betroffenen Daten einer Attacke genau untersuchen, selbst wenn die ursprünglichen Systeme von einem Cybervorfall betroffen sind.

Datenflüsse steuern: Sind die Daten mit den richtigen Merkmalen eingestuft und klassifiziert, lassen sich von der darunter liegenden Datenmanagement-Plattform automatisch Regeln durchsetzen, ohne dass der Data Owner eingreifen muss. Dadurch sinken die Risiken für menschliche Fehler.

So könnte eine Firma durchsetzen, dass bestimmte Daten wie Intellectual Property oder Finanzdaten niemals an andere Speicherorte oder externe KI-Module weitergegeben werden dürfen. Moderne Datenmanagement-Plattformen steuern den Zugriff auf diese Daten, indem sie diese automatisch verschlüsseln und sich Anwender per Access Controls und Multifaktor-Authentifizierung autorisieren müssen. Diese Zugriffskontrollrichtlinien sind ein Kernelement in NIS2, bei dem eine granularere rollenbasierte Zugriffskontrolle verlangt wird, um das Sicherheitsprinzip der geringsten Privilegien zu erreichen. Cohesity unterstützt hier das Konzept Quorum. Es ermöglicht einer Organisation, das Sicherheitsprinzip der Aufgabentrennung umzusetzen.

Auf Vorfälle reagieren: Damit eine Firma die Berichte für NIS2, DORA und DSGVO überhaupt erstellen kann, muss sie handlungsfähig sein. Bei Ransomware oder einem Wiper-Angriff wird das Licht in der Firma ausgeknipst, im sprichwörtlichen Sinn. Im Ernstfall funktioniert nichts mehr. Kein Telefon, keine E-Mail, keine Tür, geschweige denn die Website. Die IT-Teams der CIOs und CISOs werden auf diese Attacke nicht einmal reagieren können, da alle Sicherheitstools offline, Beweise in Logs und auf den Systemen verschlüsselt sind. Niemand wird sein Team zusammentelefonieren können, da VoIP nicht arbeitet. Auf Basis einer Cohesity Data Cloud Platform dagegen können die Infrastruktur-und Seucrity-Teams gemeinsam einen isolierten Cleanroom etablieren, in dem ein Notfallset an Tools und System- und Produktionsdaten liegt, um einmal einen Notbetrieb der Gesamt-IT zu schaffen. Darin liegen alle essenziellen Tools für die Security-Teams, damit diese mit dem essenziellen Incident-Response-Prozess beginnen können. Dieser Prozess ist essenziell, um richtige und aussagekräftige Berichte für NIS2, DORA und DSGVO-Verstöße zu generieren.

Vom Cleanroom aus lässt sich übrigens die Produktionsumgebung Schritt für Schritt und eng abgestimmt mit den Infrastrukturteams wiederherstellen, und zwar mit gehärteten sauberen Systemen.

Fazit

Die Regelwerke NIS2 und DORA sind wichtig für Europa und die Wirtschaft, denn sie stärken die Cyberresilienz der Firmen und Behörden. Sie spiegeln auch die Realitäten wider. KI und Service-Modelle wie Ransomware as a Service haben nicht nur die Menge von Cyberkriminalität wachsen lassen, sondern auch deren Qualität. Unsere digitale Infrastruktur muss robuster werden gegen erfolgreiche Angriffe. Dazu müssen Firmen all jene Prozesse und Workflows überarbeiten und optimieren, die mit Daten hantieren.

Mark Molyneux

DIE REGELWERKE NIS2 UND DORA SIND WICHTIG FÜR EUROPA UND DIE WIRTSCHAFT, DENN SIE STÄRKEN DIE CYBERRESILIENZ DER FIRMEN UND BEHÖRDEN.

Mark Molyneux,
EMEA CTO, Cohesity, www.cohesity.com

Netzwerktransformation

IT-INFRASTRUKTUR DER ZUKUNFT GESTALTEN

DAS MODERNSTE NETZWERK IST PRAKTISCH WERTLOS, WENN ADMINISTRATOREN UND DIE SECURITY-EXPERTEN DES UNTERNEHMENS ES NICHT MANAGEN UND SICHERN KÖNNEN.

Marcel Stadler, Product Manager SD-WAN, Open Systems, www.open-systems.com/de/

IT-Netzwerke sind das Rückgrat der digitalen Infrastruktur praktisch aller Unternehmen: ohne sie läuft meist nichts. Über die Jahrzehnte sind sie immer komplexer und verteilter geworden, was ihre Verwaltung erschwert. Gleichzeitig ist die Bedrohungslage im Cyberspace gestiegen, wodurch umfangreiche Sicherheitsmaßnahmen nötig sind, um sensible Geschäfts- und Kundendaten zu schützen. In Zeiten des Fachkräftemangels, steigender Cyberkriminalität und wachsendem Wettbewerbs müssen Unternehmen daher die Netzwerktransformation in Angriff nehmen. Nur so können sie auch dauerhaft bestehen.

Mit Netzwerken verhält es sich oft wie mit Automobilen: Gut gepflegt laufen sie über Jahrzehnte mehr oder weniger reibungslos – teils so lange, dass sie in Sachen Komfort und Sicherheit meilenweit an Boden gegenüber moderneren Modellen verlieren. Genau wie die Anschaffung eines neuen Vehikels für den privaten Endnutzer scheuen Unternehmen davor zurück, die Netzwerktransformation in Angriff zu nehmen. Die Gründe dafür sind die gleichen, nämlich unter anderem die Aversion zu ersetzen, was eigentlich noch funktionstüchtig ist. Auch die Kosten und der Aufwand einer umfangreichen Netzwerkmodernisierung lassen viele Unternehmen zurückschrecken. In vielen Organisationen kommen daher seit Jahrzehnten die gleichen Netzwerktechnologien zum Einsatz.

Das Problem daran ist, dass traditionelle Netzwerkinfrastrukturen zwar für den Moment noch ausreichen mögen, für moderne Workloads allerdings nicht die nötige Leistung bieten können. So wird es zwangsläufig bei der Integration neuer Features oder der Nutzung anspruchsvoller Anwendungen über das Unternehmensnetzwerk zu Performance-Engpässen kommen. Auch die Einführung moderner Arbeitsmodelle wie Hybrid Work und die Anbindung neuer Endpunkte ist schwierig, wenn das unterliegende Netzwerk nicht auf Expansion ausgelegt ist. Bei rückläufigen Endpunkten drohen Unternehmen zudem unnötige Kosten, wenn ihre Netzwerkinfrastruktur nicht skalierbar ist.

SASE: Ein holistischer Ansatz

Neben der puren Leistung und Flexibilität eines Unternehmensnetzwerks, muss natürlich auch die Sicherheit und die Verwaltbarkeit gewährleistet sein: Das modernste Netzwerk ist praktisch wertlos, wenn Administratoren und die Security-Experten des Unternehmens es nicht managen und sichern können, sei es aus Mangel an Mitarbeiterressourcen oder an einem zu großen Sammelsurium an Insellösungen für verschiedene Aspekte der Infrastruktur. Daher bietet es sich an, auf eine SASE (Secure Access Service Edge)-Lösung zu setzen. Das cloudbasierte Architekturkonzept vereint in sich ein softwaredefiniertes Wide Area Network (SD-WAN), inklusive aller Funktionen wie etwa der priorisierten Bandbreitenkontrolle, dem richtlinienbasierten dynamischen Routing des Traffics und der vollständigen Visibilität der gesamten Netzwerkinfrastruktur, und umfangreichen Sicherheitsfunktionen. Der Security Service Edge (SSE) einer SASE-Lösung umfasst in der Regel eine Firewall (FW), Zero Trust Network Access (ZTNA), ein Secure Web Gateway (SWG) sowie einen Cloud Access Security Broker (CASB).

Durch ihren holistischen Ansatz, der die Netzwerksicherheit mit einer softwaredefinierten Netzwerkarchitektur vereint, bieten SASE-Lösungen Organisationen alle Komponenten für eine zeitgemäße Vernetzung ihrer IT. Kleinere Unternehmen und solche, die noch mehr Mitarbeiterressourcen frei machen möchten sowie sich den Aufwand für die Umstellung auf eine hochmoderne Netzwerkinfrastruktur sparen möchten, können auch auf Managed-SASE-Angebote zurückgreifen. Manche Service Provider bieten im Zuge dessen auch ein 24/7-Management und -Monitoring des Netzwerks an.

Marcel Stadler

Darauf hat die Blockchain gewartet

MIT CONFIDENTIAL COMPUTING AUF DAS NÄCHSTE LEVEL

Die Blockchain ist einer der wichtigsten technologischen Trends der letzten Jahre. Sowohl Wirtschaft als auch Regierungen nutzen die dezentrale Datenbank, um ihre Prozesse sicherer und besser zu machen. Estland beispielsweise gehört hier zu den Vorreitern und zu den ersten „Blockchain-Regierungen". Die estnische Regierung implementierte die Blockchain bereits 2012 in ihre Datenbank, unter anderem im Sicherheits- und Gesundheitsbereich. Diese Umstellung schaffte die Grundlage für die erfolgreich eingeführte digitale Verwaltung. In diesem Land müssen Bürger fast nicht mehr aufs Amt.

Aber auch in der Wirtschaft haben viele Akteure das große Potenzial der Technologie erkannt. Die Blockchain ermöglicht beispielsweise durch ihre unveränderliche und für alle Beteiligten nachvollziehbare Datenspeicherung eine lückenlose Dokumentation und Verfolgung der Lieferkette. Umgesetzt hat das beispielsweise IBM. Deren Plattform zur Nachverfolgung der Herkunft von Lebensmitteln basiert auf der Blockchain-Technologie und ermöglicht es Verbrauchenden per Scan herauszufinden, wann und wo das Produkt, das sie gerade in den Händen halten, geerntet wurde und welchen Weg es bis zum Regal gegangen ist. Aber nicht nur Verbraucher können sich absichern, auch Unternehmen können mit dieser Transparenz beweisen, dass sie Standards, die beispielsweise 2023 im nationalen Lieferkettengesetz geregelt wurden, einhalten können.

Es gibt also viele Anwendungsbereiche und entsprechend sind die weltweiten Ausgaben für die Blockchain laut „Worldwide Blockchain Spending Guide" auch mit einer jährlichen Wachstumsrate von 48 Prozent über fünf Jahre bis 2025 hoch prognostiziert worden. Am relevantesten ist die Technologie für den Bankensektor, danach folgen die Fertigungsbranche sowie Dienstleistungen, Einzelhandel und Versicherungen.

Was genau kann die Blockchain?
Einfach ausgedrückt ist die Blockchain ein öffentliches digitales Logbuch, das eine dauerhafte Kopie von Transaktionen bereitstellt. Der Hauptvorteil einer Blockchain besteht darin, dass sie si-

cherstellt, dass die Benutzenden, die einen gemeinsamen Datensatz haben sollten, sicher sein können, dass sie dasselbe sehen. Jeder hinzugefügte Datensatz (Block) enthält einen kryptografischen Hash, mit einem Zeitstempel und Transaktionsmetadaten. Folglich kann man die Daten nicht ändern, ohne den kryptografischen Hash zu verändern, was Änderungen überprüfbar und nachverfolgbar macht. Dezentrale Finanzen oder „DeFi" ist ein Sammelbegriff, der sich auf das Konzept bezieht, Transaktionen auf öffentlichen Blockchains durchzuführen. Anstatt beispielsweise Geld über traditionelle Finanzsysteme auszutauschen, ermöglicht DeFi digitale Peer-to-Peer-Transaktionen ohne Zwischenhändler. Eines der bekanntesten Beispiele für P2P-Transaktionen ist die dezentrale Kryptowährung Bitcoin, mit der Menschen Mittel übertragen können, ohne dass ein Dritter (also zum Beispiel eine Bank) erforderlich ist. Ein weiteres Beispiel für P2P-Transaktionen ist die Peer-to-Peer-Kreditvergabe.

Es miss nicht immer die Blockchain sein

Für viele Anwendungsfälle ist die Blockchain die bestmögliche Lösung, aber manchmal reicht auch eine einfache Datenbank. Es ist wichtig zu differenzieren, was man mit dem Projekt vorhat und auf der sachlichen Grundlage der Anforderungen zu entscheiden, statt einfach blind dem Trend zu folgen.

Hackerangriffe sorgen für Unsicherheit

Im Laufe der letzten Jahre haben immer mehr Unternehmen die Blockchain-Technologie implementiert, auch weil sie sich neben der besseren Nachvollziehbarkeit von Prozessen den Schutz vor Hackerangriffen erhofft haben. Leider hat sich diese Erwartung nicht erfüllt. Im Gegenteil, seit dem Beginn des

UM DIE VORTEILE DER BLOCKCHAIN-TECHNOLOGIE NUTZEN UND AUSBAUEN ZU KÖNNEN, OHNE EIN SICHERHEITSRISIKO FÜRCHTEN ZU MÜSSEN, KÖNNEN UNTERNEHMEN UND REGIERUNGEN AUF CONFIDENTIAL COMPUTING SETZEN.

Felix Schuster,
CEO und Co-Founder, Edgeless Systems,
www.edgeless.systems

Hypes um die Technologie folgten viele Datenverstöße, beispielsweise der Angriff auf die Ronin Network-Börse oder auf die Smart Contract Blockchain-Plattform Horizon.

Laut eines Berichts der Blockchain-Datenplattform Chainalysis ist der Wert der gestohlenen Kryptowährungen zwar zurückgegangen, liegt aber mit 24,2 Milliarden Dollar im Jahr 2023 immer noch sehr hoch.

Confidential Computing

Um die Vorteile der Blockchain-Technologie nutzen und ausbauen zu können, ohne ein Sicherheitsrisiko fürchten zu müssen, können Unternehmen und Regierungen auf Confidential Computing setzen. Weshalb?

Blockchain-Systeme verwenden eine asymmetrische Verschlüsselung, um Transaktionen zu sichern. Daher ist der entscheidende Aspekt ihrer Sicherheit schon immer die Speicherung, der Schutz und die Verwendung privater Schlüssel.

Hier kommt Confidential Computing ins Spiel: Eine Möglichkeit, die Sicherheit der Blockchain zu verbessern, ist das sichere Schlüsselmanagement. Während es bisher nur möglich war, sensible Daten bei der Übertragung und beim Speichern zu verschlüsseln, können diese jetzt mit Confidential Computing auch während der Verarbeitung verschlüsselt werden. Das bedeutet, dass schützenswerte Informationen zu keinem Zeitpunkt im Klartext ausgelesen werden können, was sie vor dem unberechtigten Zugriff schützt. Bestätigt wird das durch ein vom Prozessor ausgestelltes und nicht manipulierbares Zertifikat. So ist jederzeit nachvollziehbar, was mit den Daten gemacht wurde und dass sie zu keinem Zeitpunkt entschlüsselt worden sind. Mit dieser Technologie hätten beispielsweise die Angriffe auf Ronin und Horizon verhindert werden können, weil es den Hackern nicht möglich gewesen wäre, auf die Schlüssel zuzugreifen.

Daneben ermöglicht Confidential Computing auch Blockchain-Funktionalität, die bisher weitestgehend nicht realisierbar war: die vertrauliche Ausführung von Smart-Contracts. Normalerweise sind bei einer Blockchain wie Ethereum sämtliche Transaktionen und Smart-Contract-Operationen öffentlich einsehbar. Mit Hilfe von Confidential Computing lassen sich Smart-Contracts derart ausführen, dass Eingabe- und Ausgabedaten eines Smart-Contracts geheim bleiben. Auch die Programmlogik des Smart-Contracts selbst kann geheim gehalten werden. Dies eröffnet neue Anwendungsmöglichkeiten und wird bereits von Blockchain-Protokollen wie Oasis produktiv eingesetzt.

Felix Schuster

Managed XDR

IT-SICHERHEIT IST TEAMPLAY

EINE INVESTITION IN MANAGED EXTENDED DETECTION AND RESPONSE IST FÜR EIN UNTERNEHMEN EINE INVESTITION IN DIE EIGENE SICHERHEIT UND DIE EIGENE ZUKUNFT.

Kathrin Beckert-Plewka, Public Relations Managerin, G DATA CyberDefense AG, www.gdata.de

In der digitalisierten Welt ist die IT-Sicherheit von Unternehmensnetzwerken wichtiger denn je, um die Verfügbarkeit von Daten und Ressourcen zu gewährleisten. Die IT-Systeme vor Cyberbedrohungen abzusichern, stellt viele Unternehmen aber vor eine große Herausforderung, der sie alleine nicht gewachsen sind. IT-Verantwortliche kämpfen mit dem Fachkräftemangel, begrenzten Ressourcen und fehlendem Security-Fachwissen. Daher bietet sich der Einsatz einer Managed Extended-Detection-and-Response-Lösung (kurz MXDR) an. So wird der Anbieter ein Teil des Security-Teams im Unternehmen.

Grenzen überschreitender Schutz

Klassischer Virenschutz war über eine lange Zeit der Standard in Sachen IT-Sicherheit in Unternehmen und ist bis heute eine bewährte Sicherheitslösung, die mittlerweile an Grenzen stößt. Cyberkriminelle setzen nicht nur auf Schadprogramme, um anzugreifen. Virenschutzprogramme erkennen Attacken auf der Basis des von Kriminellen eingesetzten Schadcode, dazu kommen präventive Technologien zum Einsatz. Bei der Erkennung von Malware sind die klassischen Sicherheitslösungen sehr effektiv. Bei individualisierten Angriffen sind sie hingegen aber nur begrenzt wirksam.

Diese Grenze gibt es bei Managed Extended Detection and Response nicht. Eine MXDR-Lösung verfügt über eine breit gefächerte Sensorik, um alle schädlichen Aktivitäten auf den IT-Systemen eines Unternehmens aufzudecken. So besteht die Möglichkeit, Cyberattacken schon in den Anfängen aufzuspüren und zu stoppen. Klassischer Virenschutz verfügt im Regelfall auch über eine Verhaltenserkennung, um Angriffe zu entdecken. Die Sensoren von Managed XDR sind allerdings deutlich umfangreicher. Zudem überwacht ein erfahrenes Team die IT-Systeme im Hintergrund und analysiert schädliche Vorgänge rund um die Uhr. Außerdem verfügen diese Lösungen über eine entscheidende weitere Funktion, die ein Virenschutz nicht leistet: Die Response auf schadhafte Vorgänge im Netzwerk. Ein Analystenteam reagiert umgehend, um den Schaden durch eine Attacke möglichst klein zu halten und isoliert beispielsweise einen betroffenen Endpoint vom Netzwerk.

24/7-Einsatz

Die Gewährleistung von IT-Sicherheit ist eine Rund-um-die-Uhr-Aufgabe, denn Cyberkriminelle greifen auch nachts und an Wochenenden an. Daher ist das Analystenteam einer Managed-Extended-Detection-and-Response-Lösung 24 Stunden und an sieben Tagen in der Woche aktiv, damit nicht wertvolle Zeit vergeht, bis ein laufender Angriff gestoppt wird. IT-Teams in Unternehmen können eine Rund-um-die-Uhr-Schichtabdeckung oft nicht leisten, da dies viel Personal und Aufwand in Anspruch nimmt. Im Regelfall sind die Mitarbeitenden durch das Tagesgeschäft bereits voll ausgelastet, sodass keine Zeit für IT-Sicherheit bleibt.

Ein generell großes Problem ist der Fachkräftemangel im Bereich IT-Sicherheit, der es Unternehmen erschwert, ih-

re IT-Systeme effektiv vor Cyberattacken abzusichern. Im Jahr 2022 fehlten in Deutschland mehr als 104.000 IT-Fachkräfte (Quelle: Cybersicherheit in Zahlen von G DATA CyberDefense, Statista und brand eins). Die Lücke wird immer größer, wodurch die Suche nach neuen Mitarbeitenden gerade für einen komplexen Bereich wie IT-Sicherheit sehr schwierig ist.

IT-Mitarbeitende in Unternehmen verfügen oft nicht über das tiefgreifende Security-Spezialwissen, um schädliche Vorgänge zu entdecken und detailliert zu analysieren, damit die richtige Reaktion darauf erfolgt. Wird ein Angriff in seinen Anfängen nicht entdeckt und beendet, hat dies weitreichende und fatale Folgen für das betroffene Unternehmen. Daher ist es sinnvoll, auf externe Expertise zu setzen und damit auf eine gemanagte XDR-Lösung. Das Analystenteam ist fachlich immer auf dem neuesten Stand und im ständigen Austausch mit einem internationalen Netzwerk über neue Angriffsvektoren und Cybercrime-Trends. Von dem Wissen und der Erfahrung profitieren Unternehmen, gerade wenn es um Handlungsempfehlungen abseits der reinen Überwachung geht. Diese häufige Komponente von Managed Extended Detection and Response sorgt für weitere IT-Sicherheit.

Eine Investition in MXDR ist für ein Unternehmen damit auch eine Investition in die eigene Sicherheit und die eigene Zukunft. Die Analysten werden zu einem Teil des IT-Teams eines Unternehmens und arbeiten für den Schutz der IT-Infrastruktur mit der Kernbelegschaft zusammen. Die Anschaffung einer MXDR-Lösung erhöht die IT-Sicherheit eines Unternehmens nachhaltig. Die Auswahl an unterschiedlichen Managed-XDR-Lösungen ist allerdings groß, daher sollten IT-Verantwortliche alle Angebote kritisch prüfen.

Kathrin Beckert-Plewka

CHECKLISTE FÜR DIE WAHL DES RICHTIGEN MANAGED-XDR-ANBIETERS

#1 **Managed Service:** Handelt es sich um eine reine Extended-Detection-and-Response-Lösung oder eine gemanagte Variante? Wenn die Dienstleistung nicht gemanagt wird, muss das Unternehmen ein eigenes Analystenteam beschäftigen, welches schädliche Vorgänge identifizieren und selbst sofortige Gegenmaßnahmen einleiten.

#2 **24/7-Service ist ein Muss:** Ein Anbieter sollte eine Rund-um-die-Uhr-Dienstleistung anbieten, um Cyberangriffe jederzeit zu entdecken und zu stoppen. Ansonsten ist ein umfangreicher Schutz nicht gewährleistet.

#3 **Auf die Expertise kommt es an:** Der Managed-XDR-Dienstleister sollte sehr erfahren in Sachen IT-Sicherheit sein und die Lösung selbst programmiert haben. So ist sichergestellt, dass das Analystenteam Meldungen richtig versteht und angemessen darauf reagiert.

#4 **Datenschutz:** Es ist sehr wichtig, wo der Sitz des Anbieters ist, da hiervon der geltende Datenschutz und die Gesetzgebung abhängig sind. Deutsche Dienstleister unterliegen den strengen deutschen und europäischen Datenschutzgesetzen. Sie sind außerdem dazu verpflichtet, Daten nur im Verdachtsfall einzusehen und auch nur diejenigen zu prüfen, die für die Analyse notwendig sind. Der gleiche Aspekt ist auch für den Standort der Server relevant, auf denen die Daten verarbeitet werden.

#5 **Individuelle Betreuung unerlässlich:** Der Dienstleister sollte einen Kundenservice haben, der immer erreichbar ist und einen Support in deutscher Sprache anbietet. Handlungsempfehlungen müssen leicht verständlich sein. Wichtig ist auch, dass Firmen die XDR-Lösung individuell für ihre IT-Systeme konfigurieren können und zum Beispiel festlegen, in welchen Fällen oder auf welchen Devices keine Response erfolgen soll.

#6 **Sichere Datenübertragung:** Die Kommunikation zwischen dem Agent der Managed-Extended-Detection-and-Response-Lösung (der auf den Kunden-Devices installiert ist) und der XDR-Plattform muss zwingend mehrstufig abgesichert sein. Besonders wichtig ist dies für den Response-Rückkanal zum Kunden, da sich für Unbefugte ansonsten eine Möglichkeit zum Eingreifen in die IT-Systeme des Unternehmens bietet.

#7 **Testmöglichkeit nutzen:** Es macht Sinn, die Managed-XDR-Lösung zunächst auf einer begrenzten Anzahl an Endpoints unter realen Bedingungen zu testen. So lässt sich prüfen, ob der Anbieter und die Dienstleistung zur individuellen IT-Infrastruktur passen.

Welche Cybersicherheit für die intelligente Stadt?

DIGITALE REVOLUTION UND DER ÖFFENTLICHE DIENST

In den letzten 20 Jahren hat die Digitalisierung der öffentlichen Infrastruktur unter dem Einfluss der massiven Urbanisierung und der explosionsartigen Verbreitung der Informationstechnologien die Angriffsfläche der Stadt- und Regionalverwaltungen erweitert und sie vor große Herausforderungen im Bereich der Cybersicherheit gestellt. In dieser Zeit entstand auch das Konzept der „intelligenten Stadt" oder des „intelligenten Bezirks", das durch neue Technologien, darunter ein echtes Ökosystem vernetzter Objekte, zwecks einer höheren Lebensqualität und eines besseren Ressourcenmanagements effizienter werden sollte. Doch während der Begriff „Smart City" zunächst eine eher technisch geprägte Vorstellung beschrieb, umfasst der Ausdruck heute auch rechtliche, ökologische und soziale Aspekte. Ob Tech-Stadt, Eco-Stadt oder einfach Smart City: Cyberherausforderungen stehen jedenfalls im Mittelpunkt. Denn in einer Welt, die zunehmend von digitalen Prozessen, Daten und künstlicher Intelligenz (KI) geprägt ist, entwickeln Cyberkriminelle kontinuierlich neue und raffiniertere Angriffsmethoden. Dadurch erlangt der Bedarf, sensible Infrastrukturen zu schützen, ein ganz neues Niveau.

Cyberherausforderungen einer Smart City

Städte, Gemeindeverbände, Metropolen, Landkreise: Alle sind besonders anfällig für Cybersicherheitsrisiken, da sie eine Vielzahl von Verantwortlichkeiten und Aufgaben vereinen. Die öffentliche Verwaltung modernisiert sich kontinuierlich, um zunehmend neue, vernetzte Dienstleistungen anbieten zu können. Dies eröffnet zahlreiche Szenarien. In einer Gemeinde, die zum Beispiel die Straßenbeleuchtung digitalisiert hat, melden die vernetzten Straßenlaternen den Ausfall selbstständig über ein IIoT-Gerät. Zudem hätte ein Algorithmus für vorausschauende Wartung eine Intervention auslösen können, noch bevor der Ausfall überhaupt stattgefunden hätte. Dasselbe Prinzip kommunizierender Infrastrukturen ließe sich auch auf Altglascontainer, Parkplätze oder Schwimmbäder anwenden. Diese digitale Infrastruktur ist definitiv eine Bereicherung, aber die Verknüpfung zwischen klassischen Computersystemen (IT) und operativen Systemen (OT) trägt

auch zu einer komplexeren und somit schwieriger zu schützenden Umgebung bei. Erschwerend hinzu kommt obendrein die Tatsache, dass die neuen Technologien Smart Citys nicht nur neuen Schwachstellen aussetzen, sondern sie ebenso vor Herausforderungen bezüglich der Interoperabilität stellen.

Selbst wenn man anfangs von einer Art einheitlichem Dashboard träumte, ist im Laufe der Zeit klar geworden, wie schwierig es ist, alle Steuerungssysteme in eine einzige Plattform zu vereinen. So kehren die meisten Verwaltungen zu einer pragmatischeren und weniger ehrgeizigen Vorstellung der vernetzten Stadt zurück und konzentrieren sich nun auf bestimmte Anwendungsfälle. Die Smart City wird zunehmend in kleinere Silos neu aufgeteilt. Das Ziel: IT-Technologien auf branchenspezifische Weise in die OT-Bereiche zu integrieren. Das Konzept ist demnach weniger monolithisch als früher, zumindest in Europa oder gar in Deutschland. Hier sind zum Beispiel Gemeindeverbände gemäß der KRITIS-Verordnung des BSI Betreiber einer „kritischen Dienstleistung". Als solche sind sie gesetzlich verpflichtet, unerlässliche Informationssysteme für die Betriebskontinuität der Versorgungsdienstleister (Elektrizität, Gas, Trinkwasser, Fernwärme) und der öffentlichen Infrastruktur (öffentliche Beleuchtung, Parkplätze, Transportwesen) angemessen zu schützen. Dies ist keine leichte Aufgabe.

Um die digitale Infrastruktur einer vernetzten Gemeinde zu schützen, muss eine globale Sicherheitspolitik eingeführt und dann an jedes einzelne Informationssystem angepasst werden. Und das ist häufig der Punkt, an dem es kompliziert wird. Denn neben der Vielzahl an Akteuren müssen die Kommunen auch die Herausforderungen verschiedener Netzwerkperimeter, IT und OT, zusammenführen – Netzwerke mit divergierenden Prioritäten und unterschiedlichen Sicherheitsbestimmungen.

Sollte man sich damit abfinden und dem Konzept der vernetzten Kommune sozusagen „den Stecker ziehen"? Nein, denn es gibt Möglichkeiten, die Cybersicherheit zu stärken. Und würde man sie auf Kommunen anwenden, ob in Form einer Smart City oder nicht, könnten sie weiterhin von den Vorteilen vernetzter öffentlicher Dienste profitieren.

Digitale Souveränität

Zugleich müssen öffentliche Verwaltungen aber auch europäische und nationale Vorschriften zur Cybersicherheit einhalten, darunter die DSGVO oder die Sicherheitseinstufung EU RESTRICTED auf europäischer Ebene. Im Laufe der Jahre wurde der rechtliche Rahmen, in dem sich vernetzte Gemeinden bewegen, immer umfangreicher. Das Ziel: Das Vertrauen der Benutzer in digitale Dienste soll gestärkt werden und den Rahmen für die digitale Transformation der Staaten bilden, während gleichzeitig die Sicherheit personenbezogener Daten verbessert wird. In bestimmten Situationen müssen die Kommunen also auf entsprechend qualifizierte Cybersicherheitslösungen zurückgreifen. Diese Qualifikation ist nicht nur eine simple Zertifizierung, sondern sie bescheinigt auch das Vertrauen europäischer Einrichtungen in das Sicherheitsprodukt.

DIE DIGITALE SOUVERÄNITÄT ERHÖHT DIE RESILIENZ VERNETZTER INFRASTRUKTUREN GEGEN EXTERNE BEDROHUNGEN.

Uwe Gries, Country Manager DACH, Stormshield, www.stormshield.com

Öffentliche Einrichtungen stehen großen Herausforderungen in Bezug auf die Sicherheit und die Dienstkontinuität sowie auf ihre Reputation gegenüber. Sie sind daher ein attraktives Ziel. Schließlich stellen personenbezogene und vertrauliche Daten, die im öffentlichen Sektor verarbeitet werden, für Cyberkriminelle einen nicht zu unterschätzenden Geldsegen dar. Bei gezielten Angriffen kann zudem das Motiv darin bestehen, den Zugang zu einem Dienst zu unterbrechen oder die Kommune daran zu hindern, mit ihren Bürgern zu kommunizieren. Die Methoden sind mit denen vergleichbar, die bei privatwirtschaftlichen Unternehmen beobachtet werden, aber Angriffe auf den öffentlichen Sektor kommen unter Umständen einem politischen Akt gleich, da sie gegen die Interessen der Bürger gerichtet sind. So gewinnt auch der Aspekt der digitalen Souveränität bei der Absicherung öffentlicher Dienste mehr an Bedeutung.

Mit digitaler Souveränität versteht man in Europa die Fähigkeit eines Staates und der lokalen Organisationen, die Kontrolle ihrer digitalen Informationen und Infrastrukturen sowie deren Verfügbarkeit und Integrität frei von fremden Technologieanbietern wiederzuerlangen. Im Kontext der Cybersicherheit gewinnt digitale Souveränität eine besondere Bedeutung, vor allem in geopolitischen Kontexten, wo der Zugriff auf kritische Infrastrukturen von nationalem Interesse ist. Die Abhängigkeit von extraeuropäischen Technologieanbietern kann Risiken bergen, insbesondere wenn diese Unternehmen aus Ländern stammen, die andere Datenschutz- oder Cybersicherheitsstandards haben. Die digitale Souveränität erhöht demnach die Resilienz vernetzter Infrastrukturen gegen externe Bedrohungen.

Uwe Gries

Zwischen Cyberbedrohung und Vertrauen

WIE KI IHRE VERTRAUENSWÜRDIGKEIT BEWEISEN KANN

Die Eingabe der falschen Datenquelle in ein Large Language Model (LLM) führt zur Datenvergiftung - ein weiterer Begriff, der plötzlich im Jargon der Technologieunternehmen auftaucht. Derzeit sind LLMs nicht dafür ausgelegt, Informationen zu „vergessen". In der riesigen Infrastruktur von OpenAI beispielsweise und anderen Plattformen ist es nahezu unmöglich, fehlerhafte Daten zu entfernen. Daher müssen Sicherheitsverantwortliche sicherstellen, dass LLMs von Anfang an nur die richtigen Informationen erhalten.

Woher wissen wir aber nun, was unser KI-Tool weiß, und wie können wir sicher sein, dass das Gelernte tatsächlich aus einer echten Quelle stammt?

Bei all der Aufregung über GenAI und die Zugänglichkeit des maschinellen Lernens müssen wir unsere Aufmerksamkeit auf die Sicherheit und den Wahrheitsgehalt der Daten richten, mit denen wir die Modelle füttern, und auf das, was sie letztendlich ausgeben.

KI-Sicherheitsquellcode ist keine gute Idee

Für jedes Sicherheitstool für die Erkennung von Cyberangriffen gibt es eine invasive Umgehung durch Cyberkriminelle. Bei KI besteht das größte Cybersicherheitsrisiko bereits im Training.

Ein KI-Tool kann zur Lösung repetitiver Aufgaben oder zur Optimierung bekannter Muster verwendet werden, so dass die Eingabe von bereinigtem Sicherheitscode in ein KI-Tool dazu beitragen kann, den Code effizienter zu machen. So verlockend es auch sein mag, ein KI-Modell mit dem Quellcode Ihrer Sicherheitstools zu füttern, so birgt diese Aktion doch ein unerwünschtes Risiko. Im Grunde geben Sie Ihrem KI-Modell die Werkzeuge, die es benötigt, um Ihr Sicherheitssystem zu umgehen und schließlich schädliche Ergebnisse zu erzeugen.

Dies gilt insbesondere für kreative oder innovative Anwendungsfälle, bei denen

sensible Daten in das Modell eingegeben werden. Aus offensichtlichen Datenschutz- und Sicherheitsgründen ist dies keine gute Idee. Je nachdem, wie die GenAI lernt, kann es für das Modell sehr schwierig oder sogar unmöglich sein, die Daten zu verlernen.

Richtlinien verfestigen und Linien des Codes entschärfen

Es gibt einen sehr wertvollen Anwendungsnutzen für den Einsatz von KI beim Schreiben von Low-Level-Code. In den meisten Unternehmen wird dies bereits praktiziert. Ingenieure verwenden etwa regelmäßig ChatGPT, GitHub und andere GenAI-Tools, um ihren täglichen Code zu schreiben. Insgesamt müssen technische Organisationen jedoch Richtlinien für KI-generierten Code festlegen. Sich auf das „Wissen" von GenAI zu verlassen, kann ein Sicherheitsproblem darstellen, wenn das Modell in böswilliger Absicht mit Daten gefüttert wird (um auf den Begriff der Datenvergiftung zurückzukommen).

Eine große Herausforderung ist die Fähigkeit, zwischen maschinell und von Menschen geschriebenem Code zu unterscheiden. Wenn sich herausstellt, dass der maschinengeschriebene Code problematisch ist, muss er gekennzeichnet werden, damit er schnell aus dem Verkehr gezogen oder korrigiert werden kann. Derzeit fügt sich der von der KI geschriebene Code nahtlos in den Mix ein, so dass es unmöglich ist, zu erkennen, wer oder was welchen Code geschrieben hat. Die Grenzen sind fließend und wir brauchen eine klare Abgrenzung oder einen Identifizierungsmechanismus.

Und noch etwas ist zu beachten: Code, der für sensible Aufgaben und den Umgang mit sensiblen Daten geschrieben wurde, muss sehr sorgfältig geprüft werden, bevor er von der KI optimiert wird. Sobald dieser Code übermittelt und gelernt wurde, wird er in gewisser Weise öffentlich und es ist für das Modell unmöglich, das Gelernte wieder zu verlernen. Überlegen Sie also zweimal, bevor Sie Ihre Geheimnisse mit Fremden teilen.

> „WENN MAN DER KI OFT GENUG SAGT, DASS DER HIMMEL ROSA IST, WIRD ES ZUR WAHRHEIT.
>
> **Julien Soriano, CISO, Box, www.box.com**

KI muss ihre Vertrauenswürdigkeit unter Beweis stellen

KI braucht nicht nur Zeit und Daten, um sich zu entwickeln, sondern auch wir - echte Menschen - brauchen Zeit und Informationen, um ihr zu vertrauen. Als die Cloud vor etwa zehn Jahren eingeführt wurde, waren viele Menschen skeptisch und zögerten, ihre Inhalte dort abzulegen. Heute gilt es als Status quo und sogar als Best Practice, Inhalte und sogar ganze Programme in der Cloud zu speichern. Es hat Jahre gedauert, bis wir uns daran gewöhnt haben, und dasselbe Szenario erwartet uns vermutlich auch mit KI.

Die meisten Sicherheitsexperten betrachten Zero Trust als Mantra. In den kommenden Monaten und Jahren werden CISOs daher vorrangig darauf achten, dass KI richtig eingesetzt wird und die Funktionen sicher sind. Sie werden alle grundlegenden Sicherheitsaspekte auf KI anwenden müssen, einschließlich Identitäts- und Zugriffsmanagement, Schwachstellen-Patching und vieles mehr.

Das Security AI Framework (SAIF) von Google und das AI Risk Management Framework des NIST sind beides Versuche, Sicherheitsstandards für die Entwicklung und den Einsatz von KI zu schaffen. Diese konzeptionellen Rahmen adressieren die wichtigsten Bedenken von Sicherheitsexperten und spiegeln die Idee des „Zero Trust" speziell im Bereich der KI wider.

Mit bestehenden Rahmenbedingungen und etwas Zeit wird das Vertrauen in KI als Konzept wachsen.

Julien Soriano

IT-Security

EINFACH MAL MACHEN LASSEN

In einer Welt, in der Nachrichten über Cyberattacken genauso zum Alltag gehören wie der Wetterbericht, steht der Mittelstand vor einer besonders kniffligen Herausforderung: Wie kann man mit begrenzten Budgets den ständig wachsenden Bedrohungen im Cyberspace standhalten? Nicht nur Hacker, Ransomware und Co. machen Unternehmenslenkern zu schaffen. Auch Cyberversicherungen schrauben die Sicherheitsanforderungen für eine Police immer weiter nach oben. Zu guter Letzt verschärfen neue Gesetze und die EU mit der NIS2-Richtlinie den Anspruch an die Cybersicherheit. Diese haben einen direkten Einfluss auf Unternehmen, Hersteller von Sicherheitslösungen und letztlich die gesamte Lieferkette.

Leider verfügen viele Organisationen nicht über die erforderlichen Ressourcen, das Fachwissen und die Tools, um eine wirksame Sicherheitsstrategie zu implementieren und zu betreiben. Darüber hinaus haben viele Unternehmen Schwierigkeiten, hochqualifizierte Sicherheitsexperten zu finden, um ihre IT-Infrastruktur zu schützen und auf Sicherheitsvorfälle zu reagieren.

EDR für KMU oft unverhältnismäßig

Selbst Unternehmen mit dedizierten Sicherheitsteams stehen vor der Herausforderung, die ständig wachsende Menge an Security-Daten zu verarbeiten, um potenzielle Bedrohungen rechtzeitig zu erkennen und darauf zu reagieren. Die von vielen Experten geforderten Endpoint Detection and Response-Lösungen (EDR)-Lösungen sind gerade für kleine und mittlere Unternehmen (KMU) oft nicht praktikabel und die Kosten fast unerschwinglich. Die Implementierung, der Betrieb und die Wartung solcher Lösungen erfordert erhebliche Ressourcen und Fachkenntnisse, die viele KMUs möglicherweise nicht haben. Nur eine Minderheit von Unternehmen ist überhaupt in der Lage, Sicherheitsvorfälle innerhalb kürzester Zeit zu identifizieren und zu beseitigen.

MDR als Rettungsanker

Doch es gibt eine elegante Lösung: Man betreibt EDR nicht in Eigenregie, sondern legt die eigene IT-Sicherheit in die Hände externer Dienstleister. Das sogenannte „Managed Detection and Response" erfreut sich dabei immer größerer Beliebtheit – bei Kunden und Dienstleistern.

Dahinter verbirgt sich ein Ansatz zur Sicherung von IT-Systemen und Daten vor

Cyberbedrohungen. Im Wesentlichen handelt es sich dabei um einen externen Service, der von spezialisierten Anbietern bereitgestellt wird und eine umfassende Überwachung, Erkennung und Reaktion auf potenzielle Sicherheitsvorfälle umfasst. MDR-Provider nutzen fortschrittliche Technologien wie künstliche Intelligenz, maschinelles Lernen und Verhaltensanalysen, um verdächtige Aktivitäten in Echtzeit zu identifizieren und Maßnahmen einzuleiten. Je größer dabei der Anteil von eingesetzter Künstlicher Intelligenz (KI) ist, desto kostengünstiger kann die Dienstleistung angeboten werden. Managed Detection and Response ist kein in Stein gemeißelter Service, sondern wird vom Anbieter individuell zusammengestellt.

Für wen eignet sich MDR?

MDR ist im Allgemeinen eine gute Wahl für Organisationen, die eine umfassende Sicherheitsüberwachung benötigen, ohne die gesamte Verantwortung intern zu tragen. Die externe Dienstleistung ermöglicht die Konzentration auf das Kerngeschäft, während Experten die Sicherheit überwachen.

MDR eignet sich vor allem für kleine und mittlere Unternehmen, die oft mit knappen Ressourcen für die Internetsicherheit zu kämpfen haben. MDR-Services ermöglichen es ihnen, externe Experten für die Überwachung und Reaktion auf Sicherheitsvorfälle zu nutzen, ohne ein eigenes Sicherheitsteam aufzubauen.

Aber auch Unternehmen mit komplexen IT-Infrastrukturen profitieren davon. Wenn sehr viele Endpoints, Cloud-Dienste, Netzwerke und Anwendungen im Einsatz sind, kann durch MDR (endlich) eine ganzheitliche und lückenlose Überwachung erzielt werden.

Organisationen wie Kritische Infrastruktur, die sich vor fortschrittlichen Bedrohungen schützen müssen, zählen

WENN CYBERANGRIFFE IMMER RAFFINIERTER UND ZIELGERICHTETER WERDEN, MÜSSEN UNTERNEHMEN MIT HOCHWERTIGEN SECURITY-MASSNAHMEN KONTERN.

Michael Klatte, IT-Sicherheitsexperte, ESET Deutschland GmbH, www.eset.com

ebenfalls zu den Profiteuren. MDR-Anbieter verfügen über Echtzeit-Analysten, die verdächtige Aktivitäten erkennen und darauf reagieren können. Dies ist besonders wichtig, um gezielte Angriffe und Zero-Day-Bedrohungen zu erkennen.

Vorteile von MDR

MDR-Services ermöglichen es Organisationen, Bedrohungen frühzeitiger zu identifizieren und präventive Maßnahmen zu ergreifen. Die Dienstleister verfügen über spezialisiertes Fachwissen und umfangreiche Erfahrung, die viele Organisationen intern nicht besitzen. Sie sind in der Lage, komplexe Vorfälle effektiv zu bewältigen und Sicherheitsbedrohungen zu identifizieren. Je mehr KI zum Einsatz kommt, desto vergleichsweise günstiger ist der Preis, den sich auch KMU leisten können. Organisationen können sicher sein, dass sie jederzeit vor hoch entwickelten Bedrohungen geschützt sind, ohne eigene Sicherheitsexperten einstellen und schulen zu müssen. Und: MDR unterstützt Unternehmen dabei, die Einhaltung von Datenschutz- und Sicherheitsvorschriften oder die Anforderungen von Cyberversicherungen zu gewährleisten.

Der Unterschied zwischen EDR und MDR

Endpoint Detection and Response (EDR) und Managed Detection and Response (MDR) sind zwei wichtige Ansätze in der IT-Sicherheit. Obwohl sie ähnlich klingen, besitzen sie deutliche Unterschiede.

Endpoint Detection and Response kommt auf Endpoints (Computer oder Server) zum Einsatz. Die Lösung konzentriert sich darauf, Angriffe auf spezifischen Geräten zu erkennen und einzudämmen. EDR analysiert das Unternehmensnetzwerk anhand von Funktionen wie Bedrohungserkennung, Verhaltensanalyse und Reaktion auf Sicherheitsvorfälle. Endpoint Detection and Response wird in der Regel in Eigenregie der IT-Abteilung betrieben.

Managed Detection and Response ist ein Security-Service, den externe Dienstleister für eine Organisation betreiben. Dies beinhaltet Sicherheitsüberwachung und -management über die gesamte IT-Umgebung des Auftraggebers hinweg. MDR-Anbieter können EDR-Lösungen als Teil ihres Toolkits verwenden: Deswegen ist MDR keine „Entweder-oder"-Entscheidung. Menschen spielen in dieser Dienstleistung eine wichtige Rolle, da sie Echtzeitanalysen durchführen und auf Bedrohungen reagieren können. Kostengünstige MDR-Services ersetzen bereits einen Großteil der manuellen Aktivitäten durch Künstliche Intelligenz.

Fazit

Wenn Cyberangriffe immer raffinierter und zielgerichteter werden, müssen Unternehmen mit hochwertigen Security-Maßnahmen kontern. Durch die Auslagerung der Sicherheitsüberwachung und -reaktion an spezialisierte Dienstleister für MDR erzielen Unternehmen ein starkes Sicherheitsniveau und das bei überschaubaren Kosten.

Michael Klatte

Täuschungsbasierte Erkennung

CYBERKRIMINELLE VERWIRREN UND FINDEN

Cyberkriminelle sind die Zecken im Pelz der IT-Infrastruktur. Das Eindringen der Datensauger ins Unternehmensnetz ist nicht mit hundertprozentiger Sicherheit zu verhindern. Raffinierte Angreifer sind darüber hinaus nur schwer zu entdecken, wenn sie sich erst Zugang verschafft haben. Die mittlere Verweildauer eines Angreifers beträgt im Schnitt 8 Tage. Dabei handelt es sich um die Zeit zwischen dem Zugriff eines Angreifers auf die Systeme seines Opfers und der Entdeckung der Attacke. Bedenkt man, dass Angreifer nur 16 Stunden benötigen, um das Active Directory zu erreichen, sobald sie eingedrungen sind, bleiben sie im Mittel sieben Tage unentdeckt. Dies ist mehr als genug Zeit, um einen kleineren Sicherheitsvorfall in einen wirtschaftlich schwerwiegenden zu verwandeln.

Konzentration aufs Wesentliche

Schon weil die Ressourcen eines Unternehmens nicht unbegrenzt sind, sollten sich seine IT-Sicherheitsmaßnahmen auf das wichtigste Einfallstor für Cyberkriminelle konzentrieren: E-Mails. Laut Proofpoints aktuellem „State of the Phish"-Report erlebten 86 Prozent der befragten Unternehmen in Deutschland 2023 mindestens einen erfolgreichen Phishing-Angriff. Meldungen über finanzielle Sanktionen, etwa in Form von Geldstrafen, nahmen gegenüber 2022 um 510 Prozent zu, und bei den Meldungen von Reputationsschäden gab es einen Zuwachs von 67 Prozent. Angesichts solcher Zahlen ist es wichtig für Unternehmen, avancierte E-Mail-Sicherheitstechnik mit Personalschulungen zu kombinieren, um dieses Einfallstor so gut wie möglich zu schließen.

Traditionelle Erkennungsmethoden

Aktuell verfolgen Unternehmen hauptsächlich zwei Ansätze, um erfolgreiche Angreifer zu entdecken: Sie suchen nach „bekanntermaßen schlechten" Dateien oder Netzwerkverkehr und/oder versuchen, verdächtige oder risikoreiche Aktivitäten oder Verhaltensweisen zu identifizieren. Die bekannteste Methode ist die signaturbasierte Erkennung. Im Wesentlichen geht es darum, bereits bekannte gefährliche Dateien wie Malware oder Netzwerk-Traffic von gekennzeichneten IPs oder Domains zu erkennen. Der Vorteil dieses Ansatzes ist, dass er relativ kostengünstig zu erstellen, kaufen, implementieren und verwalten ist. Der größte Nachteil ist, dass er gegen immer raffiniertere Angreifer nicht sehr effektiv ist.

DER ZWECK VON TÄUSCHUNGEN BESTEHT DARIN, ANGREIFER STOLPERN ZU LASSEN, UM IHREN NÄCHSTEN SCHRITT ZU VERHINDERN.

Miro Mitrovic,
Area Vice President DACH, Proofpoint,
www.proofpoint.com

Vor etwa 20 Jahren entstanden verhaltensbasierte Entdeckungsmethoden, um bessere Ergebnisse als mit signaturbasierter Erkennung zu erzielen. Diese probabilistischen oder risikobasierten Erkennungstechniken fanden ihren Weg in Endpunkt- und netzwerkbasierte Sicherheitssysteme sowie in SIEM, E-Mail, Benutzer- und Entitätsverhaltensanalyse (User and Entity Behavior Analytics: UEBA) und andere Sicherheitssysteme. Der Vorteil dieser Methode ist, dass sie viel nuancierter ist und bösartige Akteure finden kann, die von signaturbasierten Systemen übersehen werden. Der Nachteil ist jedoch, dass sie per Definition viele Falschmeldungen generieren kann, abhängig davon, wie sie eingestellt ist.

Zudem machen die vergleichsweise hohen Kosten für den Aufbau und den Betrieb verhaltensbasierter Systeme diese Methode für viele Unternehmen unerschwinglich. Mit dieser Feststellung sollen die gegenwärtigen und künftigen Vorteile neuerer Analysetechniken wie Künstliche Intelligenz und maschinelles Lernen nicht in Frage gestellt werden. Fortgesetzte Investitionen in verhaltensbasierte Erkennungsmethoden können sich angesichts des kontinuierlichen Wachstums von Sicherheitsdaten, Analysen und Rechenleistung auszahlen.

Erkennung überdenken

Um zu sehen, welche Methode sowohl dem signaturbasierten Ansatz als auch

dem verhaltensbasierten Ansatz überlegen ist, sollten die folgenden Fragen beantwortet werden:

#1 Wie lassen sich Bedrohungen am besten aktiv erkennen?

#2 Welche Methode ist kostengünstig, einfach zu implementieren und zu verwalten und weist eine hohe Zuverlässigkeit auf?

#3 Welcher Ansatz reduziert die Verweildauer am besten?

Die Antwort auf diese Fragen lautet „täuschungsbasierte Erkennung". Diese Technik stellt die aktive Erkennung von Bedrohungen auf den Kopf. Anstatt massenhaft Daten zu sammeln und zu analysieren, um die verräterischen Anzeichen für kriminelle Aktivitäten zu finden, werden Eindringlinge getäuscht: Für sie wird ein Minenfeld angelegt, Massen von Stolperdrähten installiert oder ein komplexes Netzwerk-Labyrinth erstellt, in dem sie die Orientierung verlieren.

Dieser Ansatz erinnert in gewisser Weise an die Idee hinter Honeypots, die in den späten 1980er Jahren aufkamen und in Clifford Stolls Buch „The Cuckoo's Egg" dokumentiert wurden. Die Kombination aus aktuellen Bedrohungstrends, den heutigen Herausforderungen bei der Erkennung und den jüngsten technologischen Veränderungen bedeutet allerdings, dass es an der Zeit ist, einen breiteren, auf Täuschung basierenden Ansatz zu überdenken.

Wer die Welt täuschungsbasierter Erkennung betritt, wird allerdings auf eine Reihe verschiedener Begriffe und Definitionen stoßen, die verwirrend und widersprüchlich sein können, darunter: Köder, Brotkrümel, Täuschung, Honeytoken, Lockvogel oder Falle. Nach meiner Ansicht bestehen zwischen den Formen der Täuschung nur nuancierte Unterschiede. Der Begriff „Täuschungen" kann dabei als Oberbegriff verstanden werden. Sie alle beziehen sich auf Arten von gefälschten Ressourcen, die Cyberkriminelle dazu bringen sollen, sich mit ihnen zu befassen. Und sie helfen den Teams, ihre Präsenz zu erkennen und Einblicke in ihre Aktivitäten und Absichten zu gewinnen.

Effektiver als Honeypots

Statt die feinen Unterschiede zwischen den genannten Begriffen zu analysieren, sollte man sich auf das eigentliche Ziel konzentrieren. Wer beispielsweise versucht, bösartige Aktivitäten im Internet zu erfassen, um Daten zu weit verbreiteten Bedrohungen zu sammeln, sollte den Einsatz von Honeypots in Betracht ziehen. Diese simulierten Hosts oder Anwendungen sind von erfahrenen Kriminellen, die in ein Unternehmensnetzwerk eingedrungen sind, zwar leicht zu erkennen und zu vermeiden, aber aufgrund ihrer Homogenität sind sie nützlich für die Sammlung von Daten für die IT-Sicherheitsforschung im großen Maßstab.

Wer jedoch das Ziel verfolgt, Eindringlinge ins Unternehmensnetz effektiver zu erkennen, zu untersuchen und ihrem Treiben Einhalt zu gebieten, sollte eher zu Täuschungen greifen. Egal, welche spezifischen Begriffe man verwendet, Täuschungen sind immer Fälschungen, die authentisch aussehen und attraktiv erscheinen, sodass Eindringlinge Schwierigkeiten haben, sie von echten Ressourcen zu unterscheiden.

Der Zweck von Täuschungen besteht darin, Angreifer stolpern zu lassen, um ihren nächsten Schritt zu verhindern. Ihr Hauptvorteil ist, dass sie vielfältig sind und sich weit im Netzwerk verteilen lassen. Dabei bleiben sie für legitime Nutzer unsichtbar – stellen für böswillige Akteure aber ein offensichtliches und verlockendes Ziel dar.

Alternative Pfade beschreiten

Den einen, alleinseligmachenden Weg, Eindringlinge zu erkennen und zu stoppen, gibt es nicht. Wem die signaturbasierte Erkennung aufgrund ihrer Defizite nicht ausreicht und verhaltensbasierte Erkennung zu kostspielig ist, sollte die Alternative täuschungsbasierter Erkennung in Betracht ziehen: Für viele Unternehmen ist es die passende Methode.

Miro Mitrovic

Sicherheitsrisiko Servicedesk

EFFEKTIVER SCHUTZ VOR ANGRIFFEN

Der Servicedesk von Organisationen spielt bei der Lösung von IT-Problemen, dem Zurücksetzen von Passwörtern und der Einrichtung von Software für die Benutzer eine wichtige Rolle. Diese Position und die damit verbundenen Berechtigungen machen Ihren Servicedesk zu einem beliebten Ziel für Cyberangriffe. Mithilfe von KI gestützten Social-Engineering-Taktiken nutzen Hacker den Schwachpunkt „Mensch" aus, um diesen zu manipulieren und so unerlaubten Zugriff auf Ihr Unternehmensnetzwerk zu erlangen.

Ohne entsprechende Schutzmaßnahmen könnte Ihr Servicedesk so unwissentlich zu einer Schwachstelle für Ihrer Organisation werden. Glücklicherweise gibt es verschiedene Strategien, um diesen Angriffspfad zu reduzieren oder zu verhindern.

Berühmt-Berüchtigte Angriffe auf Servicedesks

Social-Engineering-Angriffe werden immer häufiger, und Servicedesks sind dabei ein bevorzugtes Ziel. Bereits 2022 gaben laut Statistia 71 Prozent der befragten IT-Abteilungen an, dass sie Ziel eines Social-Engineering-Angriffs durch Vishing (Voice-Impersonation) waren - ein Anstieg um 17 Prozent im Vergleich zu den Angriffen im Jahr 2020. Wie verheerend die Auswirkungen von Social-Engineering-Angriffen in der Praxis sein können, zeigen bekannte Beispiele wie EA Games 2021 und der Angriff auf MGM Resorts 2023.

Der EA Games-Hack

Der Vorfall bei EA Games im Jahr 2021 ist ein Paradebeispiel für die Risiken, die Cyberangriffe auf den Servicedesk eines Unternehmens mit sich bringen. Nachdem sich die Hacker Zugang zu einem der internen Slack-Kanäle von EA verschafft hatten, schickten sie einem IT-Support-Mitarbeiter eine Nachricht, in der sie mitteilten, dass sie ihr Telefon auf einer Party verloren hätten und deshalb einen neuen MFA-Token benötigten, um wieder Zugang zum System zu erhalten. Sobald sie den Zugang erlangt hatten, stahlen sie Quellcodedaten von Spielen, Engines und internen Entwicklungstools und boten diese auf zahlreichen Foren zum Verkauf an. Insgesamt erbeuteten die Hacker 750 GB an Daten, darunter auch den Quellcode von FIFA 2021 und Code der Frostbite-Engine.

Der Angriff auf MGM Resorts

Im Jahr 2023 nutzte eine Hackergruppe den Namen eines Mitarbeiters von MGM Resorts auf LinkedIn und rief

Wie können Sie Ihre Servicedesk Mitarbeiter dabei unterstützen, mögliche Angreifer von echten Nutzern zu unterscheiden?
(Bildquelle: Dall-E)

dann den IT-Support von MGM an, um so an Zugangsdaten zu gelangen und sich mit diesen Credentials Zutritt zu den IT-Systemen zu verschaffen. Im Zuge dessen kam es bei dem Hotel- und Unterhaltungsriesen zu weitreichenden Störungen in zahlreichen Hotels in Las Vegas, die sich auf alles auswirkten, von Hotelzimmerschlüsseln und internen Netzwerken bis hin zu digitalen Spielautomaten und elektronischen Zahlungssystemen.

Einige Wochen später kam es noch schlimmer: Obwohl die Casinos und Hotels wieder „normal" funktionierten, gab das Unternehmen bekannt, dass die Angreifer auch in die Kundendatenbank eingedrungen waren und sich Zugang zu persönlichen Daten verschafft hatten, darunter Namen, Adressen, Geburtsdaten und (in einigen Fällen) Führerschein-, Sozialversicherungs- und Reisepassnummern.

Nach Angaben von MGM kostete der Angriff dem Unternehmen etwa 100 Millionen Dollar an Umsatzverlusten. Darüber hinaus gab das Unternehmen 10 Millionen Dollar für technische Consultants, Anwaltskosten und andere externe Berater aus, um den durch den Hack verursachten Schaden zu verringern und einzudämmen.

Best Practices zum Schutz Ihres Servicedesks

Wie die Beispiele von EA Games und MGM Resorts zeigen, ist es unerlässlich, dass Ihre Servicedesk-Mitarbeiter alle möglichen Tools und Kenntnisse zur Identifikation von solchen Angriffen haben. Mit diesen Tipps können Sie die Sicherheit Ihres Servicedesks erhöhen:

#1 Regelmäßige und kontinuierliche Schulungen zu aktuellen Angriffstechniken und Vorgehensweisen

Hacker suchen ständig nach neuen Möglichkeiten, sich unbefugten Zugang zu den Systemen und Anwendungen Ihres Unternehmens zu verschaffen - Ihr Servicedesk muss Ihnen also immer einen Schritt voraus sein. Stellen Sie sicher, dass Ihre Servicedesk-Mitarbeiter regelmäßig Schulungen zu den neuesten Social-Engineering-Methoden, Phishing-Angriffen und anderen Arten von Bedrohungen erhalten. Nur wenn diese mit aktuellem Wissen versorgt sind, können sie Ihr Unternehmen effektiv schützen. Es ist jedoch riskant (und unfair), die gesamte Verantwortung für die Prävention von Social Engineering auf die Servicedesk-Mitarbeiter zu übertragen.

#2 Automatisieren Sie den Prozess zum Zurücksetzen von Passwörtern

Kennwortresets sind für Angreifer ein beliebter Vorwand, um an Zugangsdaten heranzukommen. Angreifer geben sich oftmals als panische Mitarbeiter aus, die einen wichtigen Termin einhalten müssen oder sich in einer Notsituation befinden, weshalb der Servicedesk-Mitarbeiter unbedingt sofort einen Kennwortreset durchführen muss, damit sie rechtzeitig Zugang zum System, zur Anwendung oder zum Netzwerk Ihres Unternehmens erhalten. Oder sie geben vor erst neu im Unternehmen zu sein und im Stress der ersten Tage schon ihr Passwort vergessen haben – wem ist das noch nicht passiert?

Sie können dieses Szenario komplett unterbinden, indem Sie Passwort-Resets aus den Händen des Servicedesks nehmen und vollständig automatisieren. Mithilfe eines Tools zum Zurücksetzen von Passwörtern – entweder via Boardmitteln von Microsoft Entra ID oder Tools von Drittanbietern - können Ihre Mitarbeiter ihre Passwörter selbstständig (und sicher) zurücksetzen. Bedenken Sie nur, dass in bestimmten Fällen auch die Aktualisierung von lokal zwischengespeicherten Anmeldedaten nötig ist. Ansonsten kann solch ein Reset ohne VPN-Zugang oder Verbindung am Firmennetz doch am Servicedesk aufschlagen. Self-Service-Lösungen entlasten nicht nur Ihren Servicedesk, sondern tragen auch wesentlich zum Schutz vor Social-Engineering-Szenarien zum Thema Passwort-Resets bei.

Verifizierung von Nutzern am Servicedesk

Ihr Servicedesk wird immer ein äußerst attraktives Ziel für Hacker sein. Eine der besten Möglichkeiten, Ihre Verteidigung zu verstärken, ist die Implementierung einer Lösung, die es Ihren Servicedesk-Mitarbeitern ermöglicht, die Identität des Antragstellers sicher zu verifizieren. Lösungen wie Specops Secure Service Desk ermöglichen es Ihren Servicedesk-Mitarbeitern, mit verschiedenen Methoden - wie dem Senden eines Einmalpassworts an die mit dem Benutzerkonto verknüpfte Handynummer, E-Mail Adresse oder Verifizierung durch Vorgesetzte - zu überprüfen, ob der Nutzer wirklich derjenige ist, der er vorgibt zu sein.

Solch eine zusätzliche Sicherheitsebene kann Ihre Kollegen am Servicedesk davor schützen, Opfer ausgeklügelter Social-Engineering-Versuche zu werden.

Fazit

Abschließend lässt sich sagen, dass der Schutz des Servicedesks vor Cyberangriffen von entscheidender Bedeutung ist, um die Sicherheit Ihrer gesamten Organisation zu gewährleisten. Durch die Implementierung von regelmäßigen Schulungen, der Automatisierung von Passwort-Resets und der Einführung robuster Verifizierungsprozesse können Sie die Risiken von Social-Engineering-Angriffen und KI-gestützten Phishingversuchen erheblich minimieren. So kann Ihr Servicedesk sich wieder auf seine ursprüngliche Aufgabe konzentrieren – Ihren tatsächlichen Nutzern bei der Bewältigung von Problemen zu helfen.

Patrick Lehnis | www.specopssoft.com

Im Visier der Cyberkriminellen

WARUM GEMEINNÜTZIGE ORGANISATIONEN EIN ZIEL FÜR CYBERANGRIFFE SIND UND WIE SIE SICH SCHÜTZEN KÖNNEN

Gemeinnützige Organisationen sind häufig Ziel von Cyberangriffen mit hohem und kritischem Sicherheitsrisiko. Auf den ersten Blick mag der Trend zu Angriffen auf kleinere Organisationen widersprüchlich erscheinen, denn es gibt offensichtlich lukrativere Ziele für Cyberkriminelle als eine kleine gemeinnützige Organisation. Warum ist dieser Sektor angesichts des Risikos und des vermutlich geringen Gewinns eine interessante Zielscheibe für Angreifer?

#1 Angreifer wissen, dass gemeinnützige Organisationen weniger finanzielle Möglichkeiten und deshalb eine schwache Cyberabwehr haben

Natürlich müssen alle Unternehmen auf ihre Ausgaben achten, aber der Druck, die Kosten niedrig zu halten, ist bei gemeinnützigen Organisationen besonders groß, denn das Geld das für den eigenen Betrieb verwendet wird, kann folglich nicht mehr für die wohltätige Maßnahmen ausgegeben werden. Non-Profit-Organisationen zögern deshalb, sich zu Gemeinkostenausgaben zu verpflichten, und gleichzeitig zögern viele Unterstützer, Geld für Projekte zu spenden, die nicht direkt mit der Haupttätigkeit der jeweiligen gemeinnützigen Organisation in Zusammenhang stehen.

#2 Veraltete PCs und Betriebssysteme sowie fehlende Schulungen bedrohen die Cybersicherheit

Die Bedrohungslage in der Cybersicherheit ändert sich ununterbrochen und schnell. Computer, Betriebssysteme sowie Smartphones und Tablets müssen auf dem neuesten Stand sein, um eine ständige Flut von Sicherheitslücken zu vermeiden. Jedes angeschlossene Gerät, das nicht gepatcht wird, bietet dem Angreifer die Möglichkeit, sich Zugang zum Unternehmen zu verschaffen.

Viele gemeinnützige Organisationen sind nicht in der Lage, das Ausgabenniveau von kleinen und mittelständischen geschweige denn großen Unternehmen zu erreichen. Die finanziellen Probleme, die sich auf die Cybersicherheit beziehen, erstrecken sich auf die gesamte IT-Infrastruktur. Einige gemeinnützige Organisationen sind auf gespendete PCs angewiesen, die von Unternehmen und Privatpersonen nicht mehr benötigt und deshalb abgegeben werden. Aufgrund finanzieller Engpässe werden Schulungen zur Cybersicherheit nur oberflächlich durchgeführt – wenn sie überhaupt stattfinden. Dies erhöht das Risiko, dass gängige Taktiken wie Phishing von Angreifergruppen angewendet werden.

AUCH FÜR GEMEINNÜTZIGE ORGANISATIONEN IST EIN MODERNER CYBERSECURITY-SCHUTZ KEINE OPTION, SONDERN EIN MUSS.

Ingo Marienfeld,
Regional VP EMEA Central,
CrowdStrike,
www.crowdstrike.com

#3 Gemeinnützige Organisationen sind eine Quelle für wertvolle Daten

Gemeinnützige Organisationen sind auch aufgrund der Daten ein wertvolles Ziel für Angreifer. So verkaufen beispielsweise einige Organisationen Waren oder Dienstleistungen auf ihren Websites und speichern somit kundenbezogene Informationen in ihrem Netzwerk. Das Eindringen in einen der Server könnte Angreifer zu den Kreditkarten- und Bankdaten der Spender führen. Auch wenn diese Verkäufe nicht annähernd die Größenordnung eines Einzelhändlers wie Amazon erreichen, bietet eine gemeinnützige Organisation Angreifern die Möglichkeit, Kundendaten zu stehlen, die sie dann zum Erreichen ihrer Ziele nutzen und beispielsweise größeren, bekannteren Netzwerken ihren Wert beweisen können.

Aber nicht nur Finanzdaten sind gefährdet. Bei vielen Spendern handelt es sich um Personen oder Organisationen, deren Status und Ressourcen sie zu potenziellen Zielen machen. Der Zugriff auf ihre Daten kann Grund genug für einen Angriff auf eine gemeinnützige Organisation sein. Die Wahrscheinlichkeit, dass Mitarbeiterdaten, einschließlich persönlicher Informationen wie Sozialversicherungsnummern, Privatadressen, Telefonnummern und Bankdaten, lokal gespeichert werden, ist sehr hoch. Diese Daten können im Dark Web verkauft werden, was schwerwiegende Folgen wie Identitätsdiebstahl und finanzielle Verluste

nach sich zieht und zusätzlich Auswirkungen auf die Kreditwürdigkeit der betroffenen Mitarbeiter haben kann.

Leider gibt es viele Beispiele dafür, dass gemeinnützige Organisationen ins Visier von Cyberkriminellen geraten sind, die es auf ihre Daten abgesehen haben. So wurde beispielsweise 2019 eine der größten gemeinnützigen Organisationen in New York angegriffen, was zu einer Sicherheitsverletzung führte, bei der sensible Daten wie Namen, Adressen, Sozialversicherungsnummern, Finanzdaten, Behördenausweise, medizinische Informationen und Krankenversicherungsdaten von 1.000 Kunden offengelegt wurden.

#4 Gemeinnützige Organisationen können politische oder terroristische Ziele sein

Nicht alle Cyberangriffe sind gewinnorientiert. In einigen Fällen sind sie politisch oder sozial motiviert, insbesondere wenn es sich bei dem Ziel um eine gemeinnützige Organisation handelt. Aufgrund des Einsatzes für bestimmte Anliegen können Non-Profit-Organisationen zu einem Ziel für so genannte „Hacktivisten" oder sogar für staatlich gesponserte Cyberangriffe werden, die die gemeinnützige Organisation stören und sie an der Erfüllung ihres Auftrags hindern wollen.

#5 Gemeinnützige Organisationen können Zugang zu größeren Unternehmen bieten

Gemeinnützige Organisationen sind Teil der Software-Lieferkette und somit ist durch Anmeldedaten und Online-Zugänge der Weg zu anderen Unternehmen frei, wie zum Beispiel bei der Bestellung von Produkten und Dienstleistungen, der Abwicklung von Zahlungen und der Durchführung von Finanzgeschäften. Der Zugang zu einem schwächeren Netzwerk kann somit von Angreifern genutzt werden, um ein größeres und für die Angreifer lukrativeres Unternehmen, das geschäftliche Beziehungen zur gemeinnützigen Organisation pflegt, anzugreifen.

Fazit

Die Botschaft für gemeinnützige Organisationen ist klar: Ihre Ziele oder der wohltätige Status einer gemeinnützigen Organisation bieten keinen Schutz vor Cyberangriffen. Die Analyse zeigt vielmehr, dass diese Organisationen wichtige Ziele sind und alarmierend oft angegriffen werden.

Moderner Cybersecurity-Schutz ist somit keine Option, sondern ist ein Muss. Herkömmliche Antivirenprogramme können nicht mit dem Tempo und der Komplexität der heutigen Ransomware und Cyberangriffe mithalten.

Non-Profit-Organisationen sollten benutzerfreundliche, cloudbasierte Cybersicherheitslösungen einsetzen, die umfassender sind als AV-Tools, aber nicht das Fachwissen und die speziellen Ressourcen einer komplexen Bedrohungs-Analyseplattform erfordern. Dies gilt insbesondere für kleinere gemeinnützige Organisationen, die über ein geringeres IT-Budget und weniger Fachwissen im Bereich der Cybersicherheit verfügen. Außerdem gibt es die Möglichkeit pro bono Unterstützung und kostenlosen Zugang zu Cybersicherheitslösungen bei führenden Cybersecurity-Anbietern zu beantragen.

Ingo Marienfeld

IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

Chefredaktion: Silvia Parthier (-26)

Redaktion: Carina Mitzschke
(nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

Objektleitung:
Ulrich Parthier (-14),
ISSN-Nummer: 0945-9650

Autoren:
Kathrin Beckert-Plewka, Dennis Christ, Zeynep Dereköy, Uwe Gries, Stefan Henke, Michael Klatte, Sabine Kuch, Patrick Lehnis, Ingo Marienfeld, Miro Mitrovic, Carina Mitzschke, Mark Molyneux, Silvia Parthier, Ulrich Parthier, Detlev Riecke, André Schindler, Felix Schuster, Julien Soriano, Marcel Stadler, Alexander Summerer

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Ludwig-Ganghofer-Str. 51, D-83624 Otterfing
Tel: 08104-6494-0,
Fax: 08104-6494-22

E-Mail für Leserbriefe: info@it-verlag.de
Homepage: www.it-daily.net

Alle Autoren erreichen Sie über die Redaktion.
Wir reichen Ihre Anfragen gerne an die Autoren weiter.
Manuskripteinsendungen:
Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmteilen führen, übernimmt der Verlag keine Haftung. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Layout und Umsetzung: K.design | www.kalischdesign.de
mit Unterstützung durch www.schoengraphic.de

Illustrationen und Fotos:
Wenn nicht anders angegeben: shutterstock.com

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 31.
Preisliste gültig ab 1. Oktober 2023.

Mediaberatung & Content Marketing-Lösungen
it management | it security | it daily.net:
Kerstin Fraenzke, 08104-6494-19, fraenzke@it-verlag.de
Karen Reetz-Resch, Home Office: 08121-9775-94,
reetz@it-verlag.de
Marion Mann, +49 152-3634 1255, mann@it-verlag.de

Online Campaign Manager:
Roxana Grabenhofer, 08104-6494-21,
grabenhofer@it-verlag.de

Head of Marketing:
Vicky Miridakis, 08104-6494-15,
miridakis@it-verlag.de

Erscheinungsweise: 6 x pro Jahr

Verkaufspreis: Einzelheft 20 Euro
Jahresabopreis 100 Euro (Inland), 110 Euro (Ausland)
Probeabo 20 Euro für 2 Ausgaben
PDF-Abo 40 Euro für 6 Ausgaben

Bankverbindung:
VRB München Land eG,
IBAN: DE90 7016 6486 0002 5237 52,
BIC: GENODEF10HC

Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Abonnementservice: Eva Neff,
Telefon: 08104-6494-15, E-Mail: neff@it-verlag.de

Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Beträge.

Aktuelle Studie

SICHERHEITSBEDENKEN NEHMEN ZU

Bitdefender hat seinen aktuellen 2024 Cybersecurity Assessment Report vorgestellt. Für die Studie wurden Sicherheitsverantwortliche nach ihren Bedenken, Vorgehen und wichtigsten Herausforderungen befragt.

#1 **Künstliche Intelligenz:** Für 99 Prozent der Befragten in Deutschland sind KI-generierte Deepfakes eine Gefahr. 40,8 Prozent sehen in der Manipulation oder dem Erstellen betrügerischer Inhalte (Deepfakes) eine sehr bedeutende Gefahr.

#2 **Data Breaches:** 57,1 Prozent aller Befragten hatten in den letzten zwölf Monaten einen Fall einer Offenlegung oder eines Zugriffs auf Daten zu verzeichnen. Das ist ein Anstieg von 6 Prozent gegenüber dem Vorjahr. In Deutschland wuchs die Zahl in den letzten zwölf Monaten noch stärker von 48,5 Prozent (2023) auf 61,2 Prozent (2024) – also um 12,7 Prozent.

#3 **Druck und Wochenendarbeit:** 64,3 Prozent aller Befragten gaben an, dass sie Pläne haben, sich in den nächsten zwölf Monaten einen neuen Job suchen. Das ist ein Anstieg um 24,9 Prozent gegenüber dem Vorjahr. Der Wechselwille hat sich dabei in Deutschland mehr als verdoppelt: Von 30,9 Prozent auf 76,6 Prozent.

#4 **Identity Access Management (IAM) und Compliance:** Im Cloud-Management sehen 38,7 Prozent aller Befragten IAM als das größte Problem. Deutsche Teilnehmer sehen mehrheitlich die Schatten-IT knapp an der Spitze (35,8 %). Dahinter kommen der Mangel an Cloud-Sicherheit und der dazugehörigen Fähigkeiten mit 33,8 Prozent vor IAM und dem Sichern der Compliance mit jeweils 30,9 Prozent.

#5 **Phishing und Social Engineering:** Über 77 Prozent der deutschen Befragten sehen eine gestiegene Qualität von Social-Engineering und Phishing, was wohl mit dem plötzlichen Aufschwung der generativen KI im Zusammenhang steht.

www.bitdefender.com

Cyberkriminelle überall

da tut Hilfe not

Mehr Infos dazu im Printmagazin

itsecurity

und online auf **www.it-daily.net**


itsa EXPO CONGRESS
PLAY HARD.
PROTECT SMART.
HOME OF IT SECURITY
JETZT GRATIS-TICKET SICHERN!
22. – 24. Oktober 2024
Nürnberg, Germany
itsa365.de/itsa-expo-besuchen
NÜRNBERG MESSE